UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RD13-_____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS VERSION 5

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
Willie L. Phillips
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
willie.phillips@nerc.net

Counsel for North American Electric Reliability Corporation

January 31, 2013

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)**	**Docket No. RD13-____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS VERSION 5

The North American Electric Reliability Corporation ("NERC")[1] hereby requests that 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 following ten proposed Critical Infrastructure Protection ("CIP") Reliability Standards ("CIP Version 5") and find that they are just, reasonable, not unduly discriminatory or preferential and in the public interest:

- CIP–002–5 — Cyber Security — BES Cyber System Categorization
- CIP–003–5 — Cyber Security — Security Management Controls
- CIP–004–5 — Cyber Security — Personnel and Training
- CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
- CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
- CIP–007–5 — Cyber Security — Systems Security Management
- CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
- CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
- CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
- CIP–011–1 — Cyber Security — Information Protection

[1] NERC was certified by the Commission as the electric reliability organization ("ERO") in accordance with Section 215 of the Federal Power Act in its order issued on 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).

NERC also requests approval of the proposed definitions of terms used in the proposed CIP Version 5, the associated implementation plan, and the proposed Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs").[3] This filing also addresses all remaining standards-related issues and directives from Order No. 706.[4]

Additionally, NERC requests that CIP Version 5 become effective on the first day of the eighth calendar quarter after a final rule is issued in this docket. The requested effective date: (1) is just and reasonable; (2) properly balances the urgency to implement the standards with time allowed to develop necessary procedures, software, facilities, staffing or other relevant capabilities; and (3) allows applicable entities adequate time to ensure compliance with the requirements in accordance with Order No. 672.[5]

After a successful industry ballot with the CIP Version 5 standards achieving approval ranging from to 78.59% to 95.67%, the NERC Board of Trustees approved the CIP Version 5 standards and related documents on November 26, 2012.

Exhibit A to this filing sets forth the proposed CIP Version 5 standards and associated modifications to the Glossary of Terms used in NERC Reliability Standards. **Exhibit B** contains the Implementation Plan for CIP Version 5. **Exhibit C** contains the Standard Drafting Team Roster for Project 2008-06 Cyber Security Order 706, which is the technical team responsible for developing CIP Version 5. **Exhibit D** contains the Consideration of Comments Reports for CIP

[3] Unless otherwise specified, capitalized terms used herein have the meanings specified in the *NERC Glossary of Terms*, available at: http://www.nerc.com/files/Glossary_of_Terms.pdf.

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

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 333, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006) ("In considering whether a proposed Reliability Standard is just and reasonable, FERC will consider also the timetable for implementation of the new requirements, including how the proposal balances any urgency in the need to implement it against the reasonableness of the time allowed for those who must comply to develop the necessary procedures, software, facilities, staffing or other relevant capability.").

Version 5. **Exhibit E** contains a table of CIP Version 5 VRFs and VSLs proposed for approval and Commission guideline analyses. **Exhibit F** contains the development record for CIP Version 5. **Exhibit G** addresses the Order No. 672 Criteria for Approving Proposed Reliability Standards. **Exhibit H** contains the Consideration of Issues and Directives.

NERC is also filing the proposed CIP Version 5 standards and associated documents for approval with applicable governmental authorities in Canada.

I. EXECUTIVE SUMMARY

The White House and U.S. Congress have acknowledged that cybersecurity threats are increasing in number and sophistication. President Barack Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."[6]

Defense Secretary Leon Panetta warned that the nation is facing the possibility of a "cyber-Pearl Harbor" and is "increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid…."[7] Congress has also considered cybersecurity legislation "that would establish security standards to prevent large-scale cyber-attacks on the nation's critical infrastructure," — including the electrical grid.[8]

Recognizing the importance of the Bulk Power System, Congress has vested the ERO with the responsibility of developing mandatory Reliability Standards, including cybersecurity standards. Taking into consideration four years of experience since the first NERC CIP Cyber

[6] National Security Council, *Cyber Security*, http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.
[7] Elizabeth Bumiller and Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, The New York Times, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.
[8] Ed O'Keefe and Ellen Nakashima, *Cybersecurity Bill Fails in Senate*, The Washington Post, August 2, 2012, http://www.washingtonpost.com/world/national-security/cybersecurity-bill-fails-in-senate/2012/08/02/gJQADNOOSX_story.html.

Security Reliability Standards were implemented, as well as applicable FERC directives, NERC developed the proposed CIP Version 5 standards to better protect the reliability of the nation's Bulk Electric System ("BES")[9] from cyber-attacks.

The proposed CIP Version 5 standards were overwhelmingly supported by industry, with the industry ballot averaging nearly 90% approval. The standards also present a significant improvement over the existing CIP Version 3[10] and the Commission-approved CIP Version 4 standards.[11] For this reason, NERC seeks swift action by the Commission to approve the proposed CIP Version 5 standards as discussed in this petition.

With respect to concerns expressed by Responsible Entities regarding the transition from CIP Version 3 to Version 4 to Version 5 Reliability Standards, NERC understands that the transition could be complicated. For this reason, NERC stands ready to work with industry to address transition issues as they arise.

The proposed implementation plan for CIP Version 5, included with this filing as **Exhibit B,** provides language that would allow entities to transition from CIP Version 3 to CIP Version 5, thereby bypassing implementation of CIP Version 4 completely upon Commission approval. The proposed implementation plan specifically states:

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

[9] In this petition, the terms "Bulk Power System" and "Bulk Electric System" are used interchangeably. "Bulk Electric System" is defined in the NERC Glossary of Terms, and generally includes facilities operated at voltages at and above 100 kV. *See* NERC Glossary of Terms Used in Reliability Standards at 2. "Bulk-Power System" is defined in section 215 of the FPA, and does not include a voltage threshold. *See* 16 U.S.C. 824o(a)(1).

[10] *North American Electric Reliability* Corporation, 130 FERC ¶ 61,271 (March 31, 2010) ("In this order, we approve the modified CIP Reliability Standards, with an effective date of October 1, 2010.")

[11] *See Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (2012)(Noting CIP Version 4 Implementation date of April 1, 2014).

Prompt Commission approval of the CIP Version 5 standards and the implementation plan would reduce uncertainty among Responsible Entities regarding implementation of the CIP standards. Therefore, NERC reiterates its request for prompt Commission action approving the CIP Version 5 standards and associated implementation plan. Additionally, to help the industry implement the CIP Version 4 and 5 standards, NERC will initiate a series of industry workshops that will be presented across North America beginning in 2013.

The improvements included in CIP Version 5 reflect a maturity of the NERC CIP program. While the general framework of the proposed standards follow the organization of the previous CIP versions, a new process is introduced in proposed CIP-002-05 for identifying and classifying BES Cyber Systems according to "Low-Medium-High" impact.[12] Once BES Cyber Systems are identified, a Responsible Entity must then comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria relating to impact and other characteristics such as communications connectivity. As such, NERC and its stakeholders have proposed the most comprehensive set of mandatory cybersecurity standards ever utilized on a widespread basis in the electric industry.

Key features of the comprehensive approach taken in CIP Version 5 include:

- Utilizing a National Institute of Standards and Technology ("NIST") based approach to categorize all cyber systems which impact the BES as "Low-Medium-High" (at the system level) and requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems.

- Building on the implementation experience from prior CIP Reliability Standard versions.

- Addressing all applicable directives in Order No. 706.

- Eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System.

[12] BES Cyber Systems, discussed herein, is a proposed addition to the *Glossary of Terms used in NERC Reliability Standards*.

- Providing guidance and context within each CIP Version 5 standard.

The identification of cyber assets has evolved through the various CIP Reliability Standards versions. Building on the prior "Risk-Based Assessment Methodology" in CIP-002-3 and the "Bright-line Criteria" in CIP-002-4, the proposed CIP Version 5 standards focus on all cyber system assets that have an impact on Bulk Power System reliability, and characterizes that impact as either high, medium or low.

In Order No. 761, the Commission directed NERC to file CIP Version 5 addressing all remaining directives from Order No. 706, by March 31, 2013. With the strong support of industry, and the efforts of the diverse standard drafting team, this petition satisfies the Commission's directives two months prior to the Commission-required due date.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[13]

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
Willie L. Phillips*
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
willie.phillips@nerc.net

III. BACKGROUND AND REGULATORY FRAMEWORK

By enacting the Energy Policy Act of 2005 ("EPAct 2005"),[14] 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 electric reliability organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215 of the 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, which include requirements for the operation of existing Bulk Power System facilities and cybersecurity protection.[15]

[13] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.
[14] 16 U.S.C. § 824o (2012).
[15] *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.").

IV. JUSTIFICATION FOR APPROVAL OF THE PROPOSED RELIABILITY STANDARDS

In this section we will discuss the following: a) the basis for approval of the proposed Reliability Standards; b) significant improvements to previous CIP standards; c) new proposed Reliability Standards CIP-010-1and CIP-011-1; d) proposed definitions of glossary terms used in CIP Version 5; e) enforceability of the proposed CIP Version 5; f) VRF and VSL assignments; and g) NERC Reliability Standards Development Procedure.

This section summarizes the development of proposed CIP Version 5 and demonstrates that the proposed modifications meet the criteria for approval established by the Commission. That is, the modifications and enhancements provided in CIP Version 5 ensure that the proposed standards are just, reasonable, not unduly discriminatory or preferential and in the public interest.[16]

The proposed CIP Version 5 standards, which were overwhelmingly approved by industry, are a significant improvement over the existing CIP standards and help protect the reliability of the BES. Thus, given the strong industry support for these improvements, NERC respectfully requests that the Commission expeditiously approve the proposed CIP Version 5 standards, as presented in **Exhibit A**.

a. Basis for Approval of Proposed Reliability Standards

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

[16] *See* Order No. 672.

standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest.

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 is required to 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.[17]

The technical expertise of the ERO is derived from a standards drafting team consisting of participants that are considered experts in the cybersecurity arena. The members of the CIP Version 5 standard drafting team also provided a diversity of experience, ranging across North America, including both the continental United States and Canada. Detailed biographical information for each of the members is included with the standards drafting team roster in **Exhibit C**.

Order No. 672 sets forth the factors the Commission considers when determining whether proposed Reliability Standards meet the statutory criteria and are just, reasonable, not unduly discriminatory or preferential and in the public interest. Each of those factors is identified and addressed in **Exhibit G**.

[17] *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).

The proposed CIP Version 5 serves the important reliability goal of providing a cybersecurity framework for the identification and protection of BES Cyber Systems (discussed below) to support the reliable operation of the Bulk Power System. Generally, the framework of CIP Version 5 can be divided into two groups:

1) **Categorization of risk (based on "Low-Medium-High" impact to BES reliability)**

    - CIP–002–5 — BES Cyber System Categorization

2) **Risk mitigation lifecycle (implement, evaluate, monitor, and update)**
    - CIP–003–5 — Security Management Controls
    - CIP–004–5 — Personnel and Training
    - CIP–005–5 — Electronic Security Perimeter(s)
    - CIP–006–5 — Physical Security of BES Cyber Systems
    - CIP–007–5 — Systems Security Management
    - CIP–008–5 — Incident Reporting and Response Planning
    - CIP–009–5 — Recovery Plans for BES Cyber Systems
    - CIP–010–1 — Configuration Change Management and Vulnerability Assessments
    - CIP–011–1 — Information Protection

The proposed CIP Version 5 takes a more comprehensive approach to categorizing risk, and requires Responsible Entities to identify BES Cyber Systems, but generally maintains the cybersecurity protection framework contained in previous CIP versions. Key features of the comprehensive approach taken in CIP Version 5 include:

- Utilizing a NIST-based approach to categorize all cyber systems which impact the BES as "Low-Medium-High" (at the system level) and requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems.

- Building on the implementation experience from prior CIP versions.

- Addressing all applicable directives in Order No. 706.

- Eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System.

- Providing guidance and context within each CIP Version 5 standard.

The proposed CIP-002-5 Reliability Standard is the first step in identifying BES Cyber Systems. If a Responsible Entity does not identify any BES Cyber Systems – that ends the compliance review under proposed CIP-003-5 to CIP-011-1. However, a Responsible Entity that identifies BES Cyber Systems must comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria that characterize the impact of the identified BES Cyber Systems.

Specifically, as discussed and analyzed in detail below, proposed CIP Version 5 uses CIP-002-5 "Attachment 1 – Impact Rating Criteria" to identify three categories of BES Cyber Systems: 1) the High Impact category that covers large Control Centers, similar to those control centers identified as Critical Assets in CIP-002-4; 2) the Medium Impact category that covers generation and transmission facilities, similar to those identified as Critical Assets in CIP-002-4, along with other control centers not identified as Critical Assets in CIP-002-4; and 3) the Low Impact category that covers all other BES Cyber Systems. In addition, the Low Impact category provides protections for systems not included in CIP Version 4 (*i.e.*, CIP-002-4).

Generally, modifications to the existing CIP Reliability Standards included in the proposed CIP Version 5 standards can be described as follows:

- **CIP-002-5** will require the identification and categorization of BES Cyber Systems according to specific criteria that characterize their impact for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

- **CIP-003-5** will require approval of the documented cybersecurity policies related to CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1. CIP-003-5, Requirement 2, will require implementation of programmatic controls related to cybersecurity awareness, physical security controls, electronic access controls, and incident response to a Cyber Security Incident for those assets that have low impact BES Cyber Systems according to CIP-002-5's categorization process. The requirement that a Cyber Security Policy be "readily available" has been deleted because of general confusion around that term and because training requirements in CIP-004-5 provide for knowledge of policy. Several portions of requirements related to

information protection in previous CIP versions have been moved to CIP-011-1 and therefore deleted from CIP-003-5.

- **CIP-004-5** will require documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management. In Requirement R2, CIP-004-5 adds specific training roles for visitor control programs, electronic interconnectivity supporting the operation and control of BES Cyber Systems, and storage media as part of the handling of BES Cyber System Information. The requirements surrounding personnel risk assessments and access management were modified in response to lessons learned from implementing previous versions. Proposed CIP-004-5, Requirement R3, now specifies that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more without specifying school, work, etc., and regardless of official residence. In Requirement R4, the primary change was in combining the access management requirements from CIP-003-4, CIP-004-4, CIP-006-4 and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to improve consistency in the authorization and review process. The requirement in CIP-004-4 Requirement R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. Requirement R5 specifies revocation of access for a termination action concurrent with termination, to be completed within 24 hours.

- **CIP-005-5**, Requirement R1, focuses more on the discrete Electronic Access Points rather than the logical "perimeter." CIP-005-1 through CIP-005-4's Requirement R1.2 has been deleted from CIP Version 5. This requirement was definitional in nature and was used to bring dial-up modems using non-routable protocols into the scope of previous versions of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in CIP Version 5; therefore, there is no need for this requirement. CIP-005-1 through CIP-005-4's Requirements R1.1 and R1.3 were also definitional in nature, and they have been deleted from Version 5 as separate requirements; however, the concepts were integrated into the definitions of Electronic Security Perimeter ("ESP") and Electronic Access Point ("EAP"). CIP-005-5, Requirement R2, related to interactive remote access, is a new requirement to continue the efforts of the NERC Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

- **CIP-006-5** is intended to manage physical access to BES Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability. CIP-006-4, Requirements R8.2 and R8.3, concerning the retention of testing records, has been removed, and the retention period is specified in the compliance section of CIP-006-5.

- **CIP-007-5** will address system security by specifying technical, operational, and procedural requirements in support of protecting BES Cyber Systems against

compromise that could lead to misoperation or instability of the BES. CIP-007-5 is modified in several places to conform to the formatting approach of CIP Version 5, along with changes to address several Commission directives and to make the requirements less dependent on specific technology so that they will remain relevant for future, yet-unknown developing technologies (for example, in Requirement R3, the requirement is a competency-based requirement where the Responsible Entity must document how the malware risk is handled for each BES Cyber System, but the requirement does not prescribe a particular technical method in order to account for potential technological advancement).

- **CIP-008-5** will mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. Proposed Requirement R1 now includes an obligation to report Cyber Security Incidents within 1 hour of recognition. Requirement R2 adds testing requirements to verify response plan effectiveness and consistent application in responding to a Cyber Security Incident. Requirement R3 includes provisions for an after-action review for tests or actual incidents, along with a requirement to update the Cyber Security Incident response plan based on those lessons learned. In Requirement R3, a single timeline now combines several timelines for concurrent activities related to lessons learned and updates to recovery plans in previous CIP versions, although the total time to complete the related activities remains the same. Additionally, where previous CIP versions specified "30 calendar days" for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

- **CIP-009-5** is intended to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES. Requirement R1, adds provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized. Requirement R2 adds operational testing for recovery of BES Cyber Systems. In Requirement R3, timelines for several concurrent activities related to lessons learned and updates to recovery plans in previous versions were combined to provide one timeline, similar to CIP-009-5.

- **CIP-010-1** is a new standard that consolidates the configuration change management and vulnerability assessment-related requirements from previous versions of CIP-003, CIP-005 and CIP-007. Requirement R1 specifies the configuration change management requirements, Requirement R2 specifies the configuration monitoring requirements intended to detect unauthorized modifications to BES Cyber Systems, and Requirement R3 specifies the vulnerability assessment requirements intended to ensure proper implementation of cyber security controls along with promoting continuous improvement of cyber security posture.

- **CIP-011-1** is a new standard that consolidates the information protection requirements from previous versions of CIP-003 and CIP-007. Requirement R1

specifies information protection requirements to prevent unauthorized access to BES Cyber System Information. Requirement R2 specifies reuse and disposal provisions intended to prevent unauthorized dissemination of protected information.

All ten of the proposed CIP Version 5 standards provide a comprehensive set of requirements to protect the BES from malicious cyber-attacks. Because there are unique aspects of cyber protection for each Responsible Entity and its assets, proposed CIP Version 5 requires Bulk Power System owners, operators, and users to identify and categorize BES Cyber Systems (which are comprised of BES Cyber Assets) as described in the proposed new defined terms provided below:

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

As noted, once Responsible Entities identify BES Cyber Systems, the CIP Version 5 requirements are then applied according to the impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES, in accordance with proposed CIP-002-5.

Additionally, proposed CIP Version 5 requires responsible entities to establish plans, protocols, and controls to safeguard physical and electronic access (CIP-003-5 – CIP-011-1), to train personnel on security matters (CIP-004-5), to report security incidents (CIP-008-5), and to be prepared for recovery actions (CIP-009-5).[18]

b. CIP Version 5 presents significant improvements to previous CIP standards.

Modifying CIP-002-5 to require responsible entities to use a new approach to categorize all cyber systems impacting the BES as "Low-Medium-High" is the most significant improvement to the existing CIP Reliability Standards. This new approach effectively moves away from the CIP Version 4 "bright-line" approach of only identifying Critical Assets (and applying CIP requirements only to their associated Critical Cyber Assets), to requiring a minimum classification of "Low Impact" for all BES Cyber Systems.[19]

The shift to identifying and categorizing "High-Medium-Low" BES Cyber Systems (according to their impact on the BES) resulted from a review of the NIST Risk Management Framework for categorizing and applying security controls, a review that was directed by the Commission in Order No. 706.[20]

The following discussion is an analysis of each of the criterion included in Attachment 1 used to determine impact categories of BES Cyber Systems.

> **Criterion 1. High Impact Rating (H)**
> Each BES Cyber System used by and located at any of the following:
>
> **1.1.** Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

[18] The extensive development record includes successive drafts of the CIP Reliability Standards, the ballot pool, the final ballot results by registered ballot body members, and stakeholder comments received during the development of the proposed standards, as well as a discussion regarding how those comments were considered in developing them.
[19] Proposed CIP-003-5 through CIP-009-5 are consistent with the organization of CIP Versions 1 through 4.
[20] Order No. 706 at P 25.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4. Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

The High Impact rating category generally includes those BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Reliability Coordinator ("RC"), Balancing Authority ("BA"), Transmission Operator ("TOP"), or Generator Operator ("GOP"), as defined under the NERC Functional Model.[21]

Based on stakeholder comments, the standards drafting team made significant changes to Attachment 1, Criteria 1.1 to 1.4. Specifically, the standards drafting team tailored the definition of Control Center to refer to real-time reliability tasks for applicable functional entities from the functional model, which includes those necessary for situational awareness.

During the development process, one commenter noted that the proposed High Impact rating criteria do not consider the inter-connected nature of the BES Cyber Assets or BES Cyber Systems when defining threshold-based criteria. The standards drafting team responded that using inter-connections as an impact criterion ultimately scopes in all inter-connected systems in a single impact level. In addition, the standards drafting team recognized the concept of security zones, used heavily in the NIST Risk Management Framework, which allows the implementation of cybersecurity controls commensurate with the level of impact within a security boundary.

[21] NERC Reliability Functional Model, available at: http://www.nerc.com/page.php?cid=2%7C247%7C108.

For proposed CIP Version 5, BES Cyber Systems of all impact levels, with routable or dial-up connectivity, are required to be within a security zone that provides protection from outside influences using a posture of "mutual distrust". As such, no communication crossing the perimeter is trusted, regardless of where that communication originates. Therefore, BES Cyber Systems at High, Medium, and Low impact levels would be required to implement electronic perimeter protections for all routable and dial-up communications, regardless of inter-connectivity.

The 3,000 MW threshold in criterion 1.2 and the corresponding 1,500 MW threshold in criterion 2.13 for Control Centers performing BA functions were based on the NERC 2012 Control Performance Standard 2 Bounds Report.[22] This report lists the estimated peak demand for each BA, and the standards drafting team determined that a 3,000 MW and 1,500 MW threshold would capture roughly 90% and 96%, respectively, of the peak demand.

> **Criterion 2. Medium Impact Rating (M)**
> Each BES Cyber System, not included in Section 1 above, associated with any of the following:
>
> **2.1.** Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.
>
> **2.2.** Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

[22] NERC, *2012 CPS2 Bounds*, available at: http://www.nerc.com/docs/oc/rs/2012%20CPS2%20Bounds%20Report%20Final(Update20120419).pdf.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to

operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

- **Generation – Criteria 2.1, 2.3, 2.6, 2.9, 2.11, and 2.13 (Medium Impact Rating)**

Criteria 2.1, 2.3, 2.6, 2.9, and 2.11 of Attachment 1's Medium Impact rating category apply to Generation Owners ("GOs") and Generation Operators ("GOPs"). Criterion 2.13 is applicable to Balancing Authority ("BA") Control Centers.

Criterion 2.1 designates as Medium Impact those BES Cyber Systems that Medium Impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC Reliability Standard BAL-002, whose purpose is to ensure the BA is able to utilize its Contingency Reserve to balance resources and demand, and return Interconnection frequency within defined limits following a Reportable Disturbance.

In Criterion 2.3, the standards drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact.

Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of Interconnection Reliability Operating Limits ("IROLs") and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.

Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems ("SPS") and Remedial Action Schemes ("RAS") as medium impact. SPS and RAS's may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is needed or if it operates outside of the designed parameters. GOs and GOPs that own BES Cyber Systems for such Systems and schemes designate them as Medium Impact.

Criterion 2.11 categorizes as Medium Impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not been included in Part 1. The 1500 MW threshold omits facilities that have little impact on BES reliability, but would otherwise be captured under the newly defined term for Control Center.

Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

- **Transmission – Criteria 2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, and 2.12 (Medium Impact Rating)**

Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are applicable to Transmission Owners and Operators.

Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The 1000 MVARs value used in this criterion was a value deemed reasonable for the purpose of determining criticality by the standards drafting team. Criterion 2.2 is consistent with the criteria in CIP Version 4.

Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher, because these are single facility locations and would not have the same overall grid impact as higher rated Control Centers. Criterion 2.4 is consistent with the criteria in CIP Version 4.

It should be noted that if the collector bus for a generation plant, which is smaller in aggregate than the threshold set for generation in Criterion 2.1, is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface."[23] However, such a collector bus would not be considered Medium Impact because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

Criterion 2.5 includes BES Cyber Systems for facilities at the mid-range of BES Transmission with qualifications for inclusion if they are deemed highly likely to have

[23] NERC, *Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface* (Nov. 16, 2009), available at: http://www.nerc.com/files/GO-TO_Final_Report_Complete_2009Nov16.pdf.

significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the standards drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The standards drafting team:

- Excluded radial facilities that would only provide support for single generation facilities.
- Specified interconnection to at least three transmission stations or substations to ensure that the level of impact is consistent with a medium categorization.

The standard drafting team sought to: a) ensure inclusion of BES Transmission Facilities that perform high impact BES reliability operations, including those in large geographical areas where such Facilities operate above 200 kV, but below 300 kV; and b) provide a threshold based on existing technical studies that would be applicable to Facilities operating in the range of 200 kV to 499 kV (primarily 230 kV and 345 kV Facilities).

The total aggregated weighted value of 3,000 (utilized in criterion 2.5) was derived from weighted values related to three connected 345 kV lines or five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, without taking into account the line kV rating and a mix of multiple kV rated lines. This is in contrast to the similar criterion in CIP Version 4, which used a simple count of the lines above a certain voltage level.

Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3.

Criterion 2.7 is sourced from the NUC-001 Reliability Standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of the Nuclear Plant Interface Requirements ("NPIRs") is harmonized through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission Service Provider "for the purpose of ensuring nuclear plant safe operation and shutdown."[24] In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

Criterion 2.8 designates as Medium Impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation Owner as to the qualification of generation Facilities connected to their Transmission systems.

Criterion 2.9 designates as Medium Impact those BES Cyber Systems for those SPS, RAS, or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.[25]

Criterion 2.10 designates as Medium Impact those BES Cyber Systems for systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The standards drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding ("UFLS") systems and undervoltage load shedding ("UVLS") systems that would be subject to a

[24] NERC Reliability Standard NUC-001-2.1 — Nuclear Plant Interface Coordination, available at: http://www.nerc.com/page.php?cid=2|20.
[25] NERC Glossary of Terms at p. 63.

regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more.

Criterion 2.12 categorizes as Medium Impact those BES Cyber Systems used by and at Control Centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact. Because Control Center is a defined term, Criterion 2.12 is only applicable to the extent that a Control Center meets the standard set in the proposed definition. Control Centers that are used to perform certain functional obligations of a Transmission Operator are categorized as high impact under criterion 1.3. All other Control Centers used to perform the functional obligations of the Transmission Operator, not otherwise categorized as high impact, are categorized as Medium Impact under Criterion 2.12.

Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Criterion 3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

- **Restoration Facilities (Low Impact Rating)**

Criterion 3 would require that all remaining BES Cyber Systems (not included under Criterion 1 or Criterion 2) be designated as Low Impact. For example, under Criterion 3.4, restoration facilities are considered as Low Impact. However, such an assignment will not relieve asset owners of all CIP-related responsibilities, as would have been the case under CIP-002-4 (since only Cyber Assets with routable connectivity which are essential to restoration assets are included in CIP Version 4). With the Low Impact categorization, restoration facilities will be protected in the areas of cybersecurity awareness, physical security controls, and electronic access control, and will have obligations under CIP-003-5 regarding incident response to Cyber Security Incidents.

Restoration facilities are needed in the event of a partial or complete shutdown of facilities not used for daily activities. Notably, EPAct 2005 does not authorize NERC or the Commission to order the construction of additional generation facilities.[26] Thus, consistent with EPAct 2005, assigning a Low Impact rating to restoration facilities appropriately balances the need for timely restoration response with focused requirements for these particular types of facilities.[27]

In addition, there is no mandatory requirement that a Responsible Entity have specific restoration facilities essential to BES reliability, including Blackstart Resources and Cranking Paths. Therefore, it is imperative that NERC continues to promote availability of such resources.

[26] 16 USCS § 824o(i)(2).
[27] *See* Guidelines and Technical Basis section of CIP-002-5.

- **Control Centers (Low Impact Rating)**

Under Criterion 3.1, certain Control Centers have been designated as Low Impact, according to the impact of the Control Centers on the reliability of the BES. During the development process, several commenters noted that the proposed definition for "Control Center" would include some facilities that had very little impact on BES reliability. For example, the Control Center for a BA with a scope of less than 1500 MW has a reliability impact similar to the control system managing a generating plant of roughly the same size. Since the generating plant control system does not meet the criteria to be classified as a Medium Impact BES Cyber System, it is inconsistent to require that the BA Control Center be held to a higher impact level solely because it is a Control Center. Still, at the Low Impact rating, there are requirements for electronic perimeter protections required in proposed CIP-003-5, and the concept of "mutual distrust" attaches even to Low Impact BES Cyber Systems, which utilize either routable or dial-up communications.

c. New Proposed Reliability Standards CIP-010-1and CIP-011-1.

Proposed CIP-010-1 is a new standard that contains the configuration change management and vulnerability assessment requirements previously defined across several CIP standards in prior versions. The purpose of CIP-010-1 is to prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

Similarly, proposed CIP-011-1 is a new standard that defines information protection requirements previously defined across many standards in previous versions. The purpose of CIP-011-1 is to prevent unauthorized access to BES Cyber System Information by specifying

information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

d. Modifications to the Glossary of Terms used in NERC Reliability Standards

In proposed CIP Version 5, NERC also introduces and seeks approval of 15 newly defined terms,[28] and makes modifications to four existing definitions in Glossary of Terms used in NERC Reliability Standards.[29] The newly defined terms reduce the variable application of many existing concepts from previous CIP versions. For example, the term "Control Center" is defined under CIP Version 5, although "control center" has been used since CIP Version 1 standards were approved, and the term has been subject to differing interpretations by implementing entities.

e. Enforceability of the Proposed CIP Version 5 Reliability Standards

The proposed CIP Version 5 standards are designed to be clear and unambiguous. Indeed, CIP-002-05 was modified to address commission directives in Orders No. 706. Proposed CIP-003-5 through CIP-009-5 are generally consistent with the organization of Commission-approved CIP Versions 1 through 4. New proposed standards CIP-010-1 and CIP-011-1 also address Commission concerns and further enhance BES reliability.

In addition, the "Guidelines and Technical Basis" set forth in the CIP Version 5 standards provides Responsible Entities with sufficient information to understand their compliance obligations. The Commission should, therefore, approve CIP Version 5 as clearly enforceable.

---

[28] 1) BES Cyber Asset, 2) BES Cyber System, 3) BES Cyber System Information, 4) CIP Exceptional Circumstance, 5) CIP Senior Manager, 6) Control Center, 7) Dial-up Connectivity, 8) Electronic Access Control or Monitoring Systems ("EACMS"), 9) Electronic Access Point ("EAP"), 10) External Routable Connectivity, 11) Intermediate System, 12) Physical Access Control Systems ("PACS"), 13) Protected Cyber Assets ("PCA"), 14) Interactive Remote Access, and 15) Reportable Cyber Security Incident.

[29] 1) Cyber Assets, 2) Cyber Security Incident, 3) Electronic Security Perimeter, and 4) Physical Security Perimeter. Available at: http://www.nerc.com/docs/standards/sar/CIP_V5_Definitions_clean_4_(2012-1024-1613).pdf.

f. Violation Risk Factor and Violation Severity Level Assignments

On June 29, 2011, the Commission issued a letter order approving the VRFs and VSLs for CIP Versions 2 and 3.[30] At that time, the CIP Version 4 standards were still pending before FERC. On April 19, 2012, FERC issued a final rule approving the CIP Version 4 standards, and also approving the CIP Version 4 VRFs and VSLs, with several modifications. [31]

CIP Version 4 VSLs and VRFs served as a basis for the new CIP Version 5 VRFs and VSLs. For those requirements from CIP Version 4 that were retained in CIP Version 5 (*see* mapping document included in **Exhibit F**) NERC provides a VRF and VSL Commission Guideline Analysis, included as **Exhibit E**. NERC also proposes several new VRFs and VSLs for CIP Version 5 standards developed using the Commission guidelines.

Detailed explanations for these VRF and VSL assignments are also included in the VRF and VSL Commission Guideline Analysis in **Exhibit E**.

g. NERC Reliability Standards Development Procedure

NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of the NERC Rules of Procedure and the NERC Standard Processes Manual, which is Appendix 3A to the NERC Rules of Procedure. 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.

[30] *Letter Order Re: Violation Risk Factors and Violation Severity Levels for Version 2 and Version 3 Critical Infrastructure Protection Reliability Standards*, Docket Nos. RD10-6-001 and RD09-7-003 (June 29, 2011)
[31] *Final Rule, Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (April 19, 2012) ("Order No. 761").

The work culminating in this filing originated in FERC Order No. 706, which directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.[32]

Prior to the development of the proposed CIP Version 5 Reliability Standards, the standard drafting team developed the CIP-002-2 through CIP-009-2 standards to comply with the near-term, specific directives of FERC Order No. 706. That version of the standards was approved by FERC on September 30, 2009, with additional directives to be addressed within 90 days of the order.[33] In response, the standard drafting team developed the CIP-003-3 through CIP-009-3 standards, which were approved by FERC in March 2010.[34]

The standard drafting team for CIP Version 4 limited the scope of requirements in the development of CIP-002-4 through CIP-009-4 as an interim step to address the more immediate concerns raised in Order No. 706.[35] CIP-002-4 included "bright-line criteria" used to identify Critical Assets in lieu of an entity-defined risk-based assessment methodology. On April 19, 2012, FERC issued Order No. 761 approving CIP Version 4. In that order, the Commission also directed NERC to file the next version addressing all remaining directives from Order No. 706 by March 31, 2013.[36]

---

[32] *Id.* at P 236.
[33] *Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing*, 128 FERC ¶ 61,291 (September 30, 2009) ("September 30, 2009 Order").
[34] *Order on Compliance*, 130 FERC ¶61, 271 (March 31, 2010) ("March 31, 2010 Order").
[35] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058, at P 236 (2012) ("Order No. 761").
[36] Order No 761 at P 111.

A phased approach to meeting the directives in FERC Order No. 706 has consistently built upon prior versions of the CIP-002 through CIP-009 standards to enhance the reliability of the Bulk Electric System. Accordingly, the proposed CIP Version 5 standards build on the CIP-002-4 establishment of uniform criteria for the identification of assets.

The standards 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 before the Reliability Standard is submitted to the Commission for approval. The proposed CIP Version 5 standards were approved by the NERC Board of Trustees on November 16, 2012.

V. CIP VERSION 5 SATISFIES ALL FERC DIRECTIVES AND CONCERNS

The Commission, in Order Nos. 706 and 761, approved prior versions the CIP standards and directed NERC to address numerous issues in future versions of the CIP standards. Specifically, in Order No. 761, the Commission also directed NERC to consider the application of the NIST Risk Management Framework, regional perspective, and connectivity in developing CIP Version 5. As discussed below, proposed CIP Version 5 includes enhancements to the Commission-approved CIP standards that are responsive to all remaining Commission directives and concerns.

a. Order No. 706 Directives

In Order No. 761, the Commission directed NERC to develop the CIP Version 5 standards to address all remaining directives from Order No. 706 by March 31, 2013.

> We recognize, as numerous commenters discuss, that the current schedule for completing CIP Version 5 is aggressive. We also understand that the

> volume of industry discussion is high and we agree that industry input should not be artificially rushed or curtailed. In its reply comments, NERC indicated that it anticipates filing the Version 5 CIP Reliability Standards by the third quarter of 2012. Accordingly, to allow for sufficient time beyond what NERC estimates, we establish a deadline that is 6 months from the end of the third quarter of 2012 (i.e., March 31, 2013). NERC must also submit reports at the beginning of each quarter in which the ERO is to explain whether it is on track to meet the deadline and describe the status of its standard development efforts."[37]

The proposed CIP Version 5 addresses all applicable Commission directives in Order No. 706, and **Exhibit H** provides a summary response for each of the Commission's directives and guidance statements.

b. Application of NIST Risk Management Framework

In Order No. 706, the Commission directed NERC to apply applicable features of the NIST Risk Management Framework to CIP Version 5. Order No. 761 also urged NERC to review relevant NIST standards for guidance in developing effective cybersecurity standards for the electric industry.[38]

Pursuant to Order Nos. 706 and 761, the standards drafting team for CIP Version 5 reviewed the NIST Risk Management Framework and incorporated five key features:

1. ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection;

2. a tiered approach to security controls, which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System;

3. tailoring protection to the mission and operating environment (*e.g.*, communications connectivity) of the cyber systems subject to protection;

[37] Order No 761 at P 111.
[38] Order No. 761 at P 94 (The Commission stated: "We view the approach of incorporating these applicable features of the NIST Framework into the CIP Reliability Standards as a positive step in improving cyber security for the Bulk-Power System.").

4. the concept of the BES Cyber System, and

5. the inclusion of "Assess" and "Monitor" steps by adding requirement language for "identifying, assessing, and correcting" deficiencies in controls as part of the requirements' expected performance.

Proposed CIP Version 5 achieves reliability excellence by incorporating the above features of the NIST Risk Management Framework.[39] The NIST Risk Management Framework defines "risk" as a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.[40] NIST further explains that this risk management process "changes the traditional focus of [Certification and Accreditation] as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions." [41]

Indeed, both NERC and the Commission have acknowledged the importance of identifying and correcting risks to the Bulk Power System. NERC has stated in prior proceedings that, "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."[42] In its order accepting NERC's

[39] In 2013, NERC Compliance Operations will be revising all Reliability Standard Audit Worksheets ("RSAW"), including the RSAWs for CIP Version 5. To incorporate the NIST Risk Management Framework into CIP Version 5, the standards drafting team discussed the importance of synchronizing the "identify, assess, and correct" language with associated RSAWs, and developed a sample RSAW for proposed CIP-006-5. The sample RSAW was posted for informational purposes only and the Commission is *not* being asked to approve the sample RSAW, which is available at: http://www.nerc.com/page.php?cid=3|404.
[40] *Id*. at FN 8.
[41] NIST, Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, at p. 2.
[42] *NERC Petition Requesting Approval of New Enforcement Mechanisms and Submittal of Initial Find Fix and Track (FFT) Informational Filing*, at p.1, Docket No. RC11-600 (2011) (*Emphasis added*).

Find, Fix, and Track approach to enforcement, FERC agreed with NERC's assessment, stating that it "applaud[s] NERC for proposing a format that will help it and the Regional Entities focus their resources on issues that pose the greatest *risks* to reliability."[43]

Consistent with the NIST Risk Management Framework and the Commission's guidance in prior orders, the CIP Version 5 standard drafting team incorporated within several standards (*e.g.*, proposed CIP-003-5) a requirement that Responsible Entities implement cyber policies in a manner to "identify, assess, and correct" deficiencies. The "identify, assess, and correct" language is included as a performance expectation in the requirements, not as an enforcement component. An example of this language follows below:

> Each Responsible Entity shall implement**,** in a manner that identifies, assesses, and corrects deficiencies**,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table].

The implementation of certain CIP Version 5 requirements in a manner to "identify, assess, and correct" deficiencies emulates the *FERC Policy Statement on Penalty Guidelines*, where the Commission clarified that "[a]chieving compliance, not assessing penalties, is the central goal of the Commission's enforcement efforts."[44] The *FERC Policy Statement on Penalty Guidelines* also highlights the characteristics of an effective organization compliance program, which include "(1) [exercising] due diligence to prevent and detect violations; and (2) [promoting] an organizational culture that encourages a commitment to compliance with the law."[45]

---

[43] *Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing*, 138 FERC ¶61,193 (March 15, 2012) at P 40. (*Emphasis added*).
[44] *Revised Policy Statement on Penalty Guidelines*, 132 FERC ¶ 61,216 at P 110 (2010).
[45] *Id*.

The *FERC Policy Statement on Penalty Guidelines* further explains that the promotion of an "organizational culture that encourages a commitment to compliance" requires an organization to establish standards and procedures to prevent and detect violations.[46] Therefore, the organization's governing authority should be knowledgeable of the compliance program and exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program by assigning a specific individual(s) within high-level personnel overall responsibility for the compliance program. To that end, the *FERC Policy Statement on Penalty Guidelines* requires organizations to "periodically assess the *risk* of violations and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of violations identified through this process."[47]

This creation of an organizational culture of compliance, with an emphasis on assessing risk, is consistent with the approach taken in CIP Version 5 and avoids a "check-the-box" mind-set that would consume valuable industry resources without any benefit to BES reliability. For example, proposed CIP-003-5 requires Responsible Entities to identify a CIP Senior Manager. Rather than verifying that a single name appears on a document, CIP-003-5 seeks to verify that the *purpose* of the requirement is being achieved – that a CIP Senior Manager is indeed managing the implementation of CIP Version 5.

This is an example of how the lessons learned over the past four years are reflected in CIP Version 5, which includes high-level personnel (*i.e.*, the CIP Senior Manager) assessing risk. Thus, CIP Version 5 builds on the implementation and audit lessons from prior versions and is consistent with the *FERC Policy Statement on Penalty Guidelines.*

[46] FERC Penalty Guidelines, Chapter 1, Part B - Disgorging Gain From Violations and Effective Compliance Program, §1B2.1, Effective Compliance Program.
[47] http://www.ferc.gov/whats-new/comm-meet/2010/091610/M-1.pdf. (*Emphasis added*).

c. Regional Perspective

In Order No. 761, the Commission expressed a concern that a lack of a regional review for the identification of cyber assets might result in a reliability gap. However, CIP Version 4 adopted "bright-line" criteria for Critical Asset identification, which the Commission agreed may obviate the need for a regional review.[48] Building on the CIP Version 4 approach, the proposed CIP-002-5, Attachment 1 – Impact Rating Criteria was developed in consideration of a Wide Area view and eliminates the need for regional review.

However, in the event that there are BES Cyber Systems that NERC and the Regional Entities determine should be treated as critical, but do not meet the CIP Version 5 criteria, NERC has the authority under Section 810 of the NERC Rules of Procedure to issue a Level 2 (Recommendation) or Level 3 (Essential Action) notification. Section 810 of the NERC Rules of Procedure provides the following:

> **810. Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions**
>
> **1.** Members of NERC and Bulk Power System owners, operators, and users shall provide NERC with detailed and timely operating experience information and data.
>
> **2.** In the normal course of operations, NERC disseminates the results of its events analysis findings, lessons learned and other analysis and information gathering to the industry. These findings, lessons learned and other information will be used to guide the Reliability Assessment Program.
>
> **3.** When NERC determines it is necessary to place the industry or segments of the industry on formal notice of its findings, analyses, and recommendations, NERC will provide such notification in the form of specific operations or equipment Advisories, Recommendations or Essential Actions:

[48] Order No. 761 at P PP 103 and 104 ("We believe that there is less need for external review where application of bright line criteria results in an objective, consistently applied approach to the identification of cyber assets.").

3.1 Level 1 (Advisories) – purely informational, intended to advise certain segments of the owners, operators and users of the Bulk Power System of findings and lessons learned;

3.2 Level 2 (Recommendations) – specific actions that NERC is recommending be considered on a particular topic by certain segments of owners, operators, and users of the Bulk Power System according to each entity's facts and circumstances;

3.3 Level 3 (Essential Actions) – specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System to take to ensure the reliability of the Bulk Power System. Such Essential Actions require NERC Board approval before issuance.

4. The Bulk Power System owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) notifications apply are to evaluate and take appropriate action on such issuances by NERC. Such Bulk Power System owners, operators, and users shall also provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions in accordance with the reporting date(s) specified by NERC.

5. NERC will advise the Commission and other Applicable Governmental Authorities of its intent to issue all Level 1 (Advisories), Level 2 (Recommendations), and Level 3 (Essential Actions) at least five (5) business days prior to issuance, unless extraordinary circumstances exist that warrant issuance less than five (5) business days after such advice. NERC will file a report with the Commission and other Applicable Governmental Authorities no later than thirty (30) days following the date by which NERC has requested the Bulk Power System owners, operators, and users to which a Level 2 (Recommendation) or Level 3 (Essential Action) issuance applies to provide reports of actions taken in response to the notification. NERC's report to the Commission and other Applicable Governmental Authorities will describe the actions taken by the relevant owners, operators, and users of the Bulk Power System and the success of such actions taken in correcting any vulnerability or deficiency that was the subject of the notification, with appropriate protection for Confidential Information or Critical Energy Infrastructure Information.

Level 3 Alerts allow NERC (following NERC Board of Trustees approval) to require that specific actions that NERC has determined are essential for certain segments of owners, operators, or users of the Bulk Power System be taken to ensure the reliability of the Bulk Power

System. Additionally, Rule 810 states that Bulk Power System owners, operators, and users to which Level 2 (Recommendations) and Level 3 (Essential Actions) Alerts apply shall provide reports of actions taken and timely updates on progress towards resolving the issues raised in the Recommendations and Essential Actions consistent with reporting dates specified by NERC. Therefore, NERC can use Level 2 Recommendations and Level 3 Essential Actions to address assets that NERC and Regional Entities later determine should be treated as a higher impact level than would otherwise be categorized under the CIP Version 5 impact criteria.

d. Connectivity

In Order No. 761, the Commission noted that the criteria adopted for the purpose of identifying assets under CIP-002-5 should include a cyber asset's "connectivity."[49]

> We also agree with SPP RE that the CIP Reliability Standards should consider communication paths between a given cyber asset and other assets that support a reliability function. As noted by SPP RE, cyber security standards that categorize cyber systems based upon the size or scope of the assets that they control "fail to consider the interconnectivity of the BES Cyber Systems and the potential for a small control center system to be used as a vector of attack against a larger control center system." …The Commission agrees that cyber connectivity is important to address when developing future versions of the CIP Reliability Standards. That being said, we acknowledge the concern of Trade Associations that the "connectivity" and "weakest link" concepts could possess different meanings to various stakeholders. Thus, addressing connectivity should include reaching a common understanding of the term. Further, we understand and agree with the Trade Associations' concern that protection should be applied in a reasonable manner.

Order No. 761at P 88. (Citations omitted).

The CIP Version 5 standards drafting team agreed with the Commission that connectivity is a relevant consideration for the application of cybersecurity controls, and comprehensively incorporated connectivity throughout CIP Version 5 by utilizing a "mutual distrust" posture, by

[49] Order No. 761at PP 88 - 91.

eliminating any connectivity-based exclusions under CIP-002-5, Attachment 1, and thorough inclusion of connectivity and other characteristics in the applicability of the CIP Version 5 requirements.

If connectivity were used as an initial impact criterion, it could potentially expand the CIP Version 5 standards to a significant number of non-jurisdictional assets, such as interconnected distribution systems (*e.g.*, smart grid), market systems, and business systems. Furthermore, using connectivity as a basis for categorizing impact could continue the unintended consequences related to eliminating connectivity in certain circumstances, resulting in a decreased situational awareness ability and increased costs associated with not being able to readily gather data or perform necessary maintenance. Accordingly, proposed CIP Version 5 addresses the Commission's concerns related to connectivity throughout the proposed CIP Version 5 standards.

Specifically, the standards drafting team determined that, while connectivity may affect the ability to remotely access a BES Cyber System, the impact to BES reliability is determined by the electrical characteristics of a BES asset, not by the connectivity of an associated BES Cyber System. This does not, however, diminish the importance of connectivity, as the applicability of requirements consider connectivity in proposed CIP-003-5 through CIP-011-1.

Connectivity does not inform BES impact, even if it affects likelihood or risk. The role connectivity plays in affecting likelihood or risk of access or compromise to a Cyber Asset associated with a BES Cyber System is a significant reason why connectivity is more appropriately considered in the applicability of requirements throughout the CIP Version 5 standards. To illustrate, the loss of 1000 MW of Load would have the same impact to the BES regardless of whether it stemmed from the compromise of an asset's BES Cyber System (that is

routably connected) or from the compromise of an asset's BES Cyber System that has no connectivity whatsoever. The likelihood or risk of compromise to the former is arguably higher, but the impact to BES reliability—in the instant case, 1000 MW—would be the same under both circumstances. Indeed, the likelihood or risk of compromise *is* addressed by the applicability of additional requirements where routable connectivity is used, not by characterizing the BES Cyber System to a higher impact category.

In addition, Order No. 761 encourages NERC to consider the benefits of a "mutual distrust" posture as directed by the Commission in Order No. 706.[50]

> Recognizing the importance of addressing cyber connectivity in future versions of the CIP Reliability Standards, we encourage NERC to consider the benefits of a "mutual distrust" posture, or similar strategies, put forth by the ISO/RTO Council and as directed by the Commission in Order No. 706. In Order No. 706, the Commission used the term "mutual distrust" to denote how "outside world" systems are treated by those inside the control system. Specifically, a mutual distrust posture requires each responsible entity that has identified critical cyber assets to protect itself and not trust any communication crossing an electronic security perimeter, regardless of where that communication originates.
>
> Applying electronic security perimeter protections "of some form" to bulk electric system cyber systems covered by the CIP Reliability Standards will support the adoption of a "mutual distrust" posture. This posture will encourage asset owners and operators to employ sound network architectural design, thus segmenting their systems into distinct security zones protected by managed interfaces that will allow only trusted access. The managed interfaces, or electronic security perimeter access points, are intended to restrict or prohibit network access and information flow to bulk electric system cyber systems covered by the CIP Reliability Standards from unidentified, unauthenticated, and unauthorized connectivity to ensure security. Multiple electronic security perimeters can be established to protect cyber assets and adopted as part of a defense in depth strategy to limit the propagation of a threat.

Order No. 761at PP 89-90. (Citations omitted).

[50] Order No. 761 at P 89.

"Mutual distrust" signifies how "external" cyber assets are treated by those cyber assets local to the BES Cyber System. "Mutual distrust" also requires each Responsible Entity that has identified BES Cyber Systems to protect against any communication crossing an ESP, regardless of where the communication originates. As noted above, BES Cyber Systems of all impact levels, with routable or dial-up connectivity, are required to be within a security zone that provides protection from outside influences using a posture of "mutual distrust". Since, under CIP Version 5, BES Cyber Systems for "High-Medium-Low" impact levels are now required to implement electronic perimeter protections "of some form" for all routable and dial-up communications, the "mutual distrust" posture is implemented for all BES Cyber Systems.

The Commission also stated in Order No. 761 that, "we support the elimination of the blanket exemption for non-routable connected cyber systems as highlighted in NERC's comments. A continued blanket exemption in CIP Version 5 would not adequately address risk."[51] The Commission added that, "we support the concept of applying electronic security perimeter protections 'of some form' to all bulk electric system cyber systems."[52]

The standards drafting team for CIP Version 5 agreed that applying ESP protections "of some form" to BES Cyber Systems supports the "mutual distrust" posture even for low impact BES Cyber Systems that use routable or dial-up communications.[53] Ultimately, using "mutual distrust" is equally efficient and effective as considering connectivity as a basis for informing the impact categorization of BES Cyber Systems. Thus, the implementation of a "mutual distrust" posture for high, medium, and low impact BES Cyber Systems, connected using routable or dial-up communications, improves security above what is required under CIP Versions 1 through 4.

[51] Order No. 761 at P 86.
[52] Order No. 761 at 87.
[53] Order No. 761 at 87.

Moreover, in response to stakeholder comments during development, proposed CIP-003-5, requirement R2, was added so that Responsible Entities are required to document and implement perimeter-type security controls to segment Low Impact BES Cyber Systems from public (or other less trusted) network zones and to prevent access to an aggregation of low impact BES Cyber Systems. The intent of this enhancement is to mitigate the risks associated with the aggregation of Low Impact BES Cyber Systems, in order to avoid a potential increase in the overall level of impact to the BES.

Additionally, because electronic perimeter protections are now required for BES Cyber Systems (with specific requirements for High and Medium impact categories and programmatic requirements for Low impact) CIP Version 5 adequately addresses connectivity.

VI. SUMMARY OF THE RELIABILITY STANDARD DEVELOPMENT PROCEEDINGS

The development record for proposed CIP Version 5 is summarized below. **Exhibit D** contains the Consideration of Comments Reports created during the development of the Reliability Standards. **Exhibit F** contains the complete record of development for proposed CIP Version 5.

Three drafts of CIP Version 5 were posted for industry comment during the development period before being approved during recirculation ballot in draft 4. The first draft of the standards was posted for comment from November 7, 2011, through January 6, 2012. This period included twelve initial ballots (one each for the ten standards in proposed CIP Version 5, the associated definitions, and the implementation plan) that were conducted from December 16,

2011, through January 6, 2012, and they resulted in industry approvals between 22.09 and 42.06 percent.[54]

The CIP Version 5 standards drafting team then focused its efforts on preparing the next draft in response to comments received. The second draft of CIP Version 5 was posted for comment from April 12 through May 21, 2012. This period included successive ballots that were conducted from May 11 through May 21, 2012, and resulted in industry approvals between 37.37 and 67.19 percent.[55]

The standards drafting team made further refinements in an effort to address unresolved issues and to develop industry consensus in response to the second posting. The third draft of CIP Version 5 was posted for comment from September 11 through October 10, 2012. This period included successive ballots that were conducted from October 1 through October 10, 2012, and they resulted in industry approvals between 74.85 and 94.00 percent.[56]

Recirculation ballots, which constituted draft four of CIP Version 5, were conducted from October 26 through November 5, 2012, and resulted in industry approvals between 78.59 and 95.53 percent.[57] The NERC Board of Trustees approved the proposed CIP Reliability Standards on November 16, 2012.

VII. CIP VERSION 5 IMPLEMENTATION PLAN

The proposed CIP Version 5 implementation plan was overwhelmingly passed by the registered ballot body with 94.91% approval. Yet, until the Commission takes action on CIP Version 5, there may be uncertainty for Responsible Entities transitioning from CIP Version 3 to

[54] http://www.nerc.com/docs/standards/sar/Standards_Announcement_2008-06_ballot_results_010612_final.pdf.
[55] http://www.nerc.com/docs/standards/sar/Succ_Ballot_Results_2008-06_CIPV5_20120522_060612.pdf.
[56] http://www.nerc.com/docs/standards/sar/Succ_Ballot_Results_2008-06_CIPV5_20121012_rev1.pdf.
[57] http://www.nerc.com/docs/standards/sar/2008-06_CIPV5_Recirc_NPB_Results_Announc_110712_final.pdf.

CIP Version 4 to CIP Version 5. This uncertainty stems from industry stakeholders not knowing whether the Commission will act on CIP Version 5 prior to the CIP Version 4 effective date, April 1, 2014, which would trigger compliance obligations for Responsible Entities.

NERC will work with the industry on any potential implementation challenges. However, language included in the proposed implementation plan could help alleviate some of the uncertainty among industry. This language provides:

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.

With prompt Commission approval of the CIP Version 5 standards and the associated implementation plan, CIP Version 3 will be extended until CIP Version 5 becomes operative, bypassing implementation of CIP Version 4.

While there is significant support for the CIP Version 5 implementation plan, NERC stands ready to implement CIP Version 4, if the Commission does not act before April 1, 2014. NERC will work with industry stakeholders to address any transition issues as they arise; although NERC urges the Commission to approve the proposed CIP Version 5 standards and the associated implementation plan as soon as possible.

Prompt approval of CIP Version 5 will provide much needed clarity for Responsible Entities transitioning from CIP Version 3 to CIP Version 4 to CIP Version 5, and the improvements contained in CIP Version 5 will provide an enormous benefit to BES reliability. However, if the Commission determines that prompt approval of CIP Version 5 is infeasible, NERC respectfully requests that a timeframe for anticipated action be provided, so that NERC and industry may develop a reasonable plan to move from CIP Version 3 to CIP Version 4 to CIP Version 5.

VIII. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission approve the proposed CIP Version 5 Reliability Standards and related documents in accordance with this petition and Order Nos. 706 and 761.

Respectfully submitted,

/s/ Willie L. Phillips

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
Willie L. Phillips
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
willie.phillips@nerc.net

Counsel for North American Electric Reliability Corporation

Dated: January 31, 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 31st day of January, 2013.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

Exhibit A

1.) Proposed CIP Version 5 Reliability Standards submitted for Approval
2.) Associated Modifications to the Glossary of Terms used in NERC Reliability Standards

Exhibit A

1.) Proposed CIP Version 5 Reliability Standards submitted for Approval

A. Introduction

1. Title: Cyber Security — BES Cyber System Categorization

2. Number: CIP-002-5

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-002-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

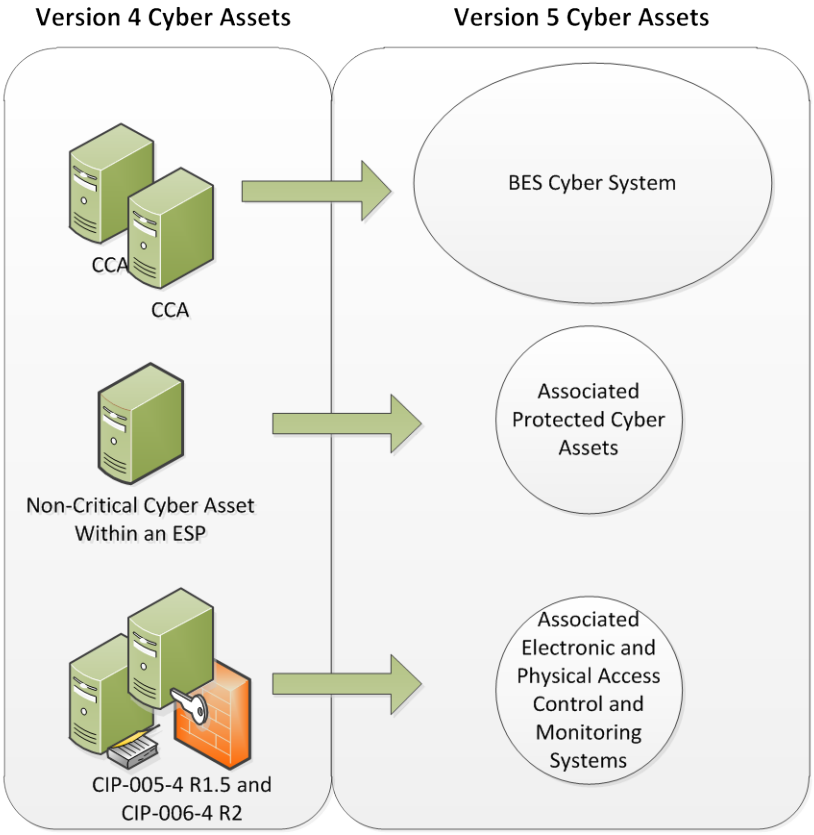
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and

2.2 Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection.

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

2.6. Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the generation Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1 or 2.3.

2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

2.10. Each system or group of Elements that performs automatic Load shedding under a common control system, without human operator initiation, of 300 MW or more implementing undervoltage load shedding (UVLS) or underfrequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

2.11. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Generator Operator for an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above.

2.13. Each Control Center or backup Control Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. .

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

    - Excluded radial facilities that would only provide support for single generation facilities.

    - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

    - 230 kV –> 700 MVA

    - 345 kV –> 1,300 MVA

    - 500 kV –> 2,000 MVA

    - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

    - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

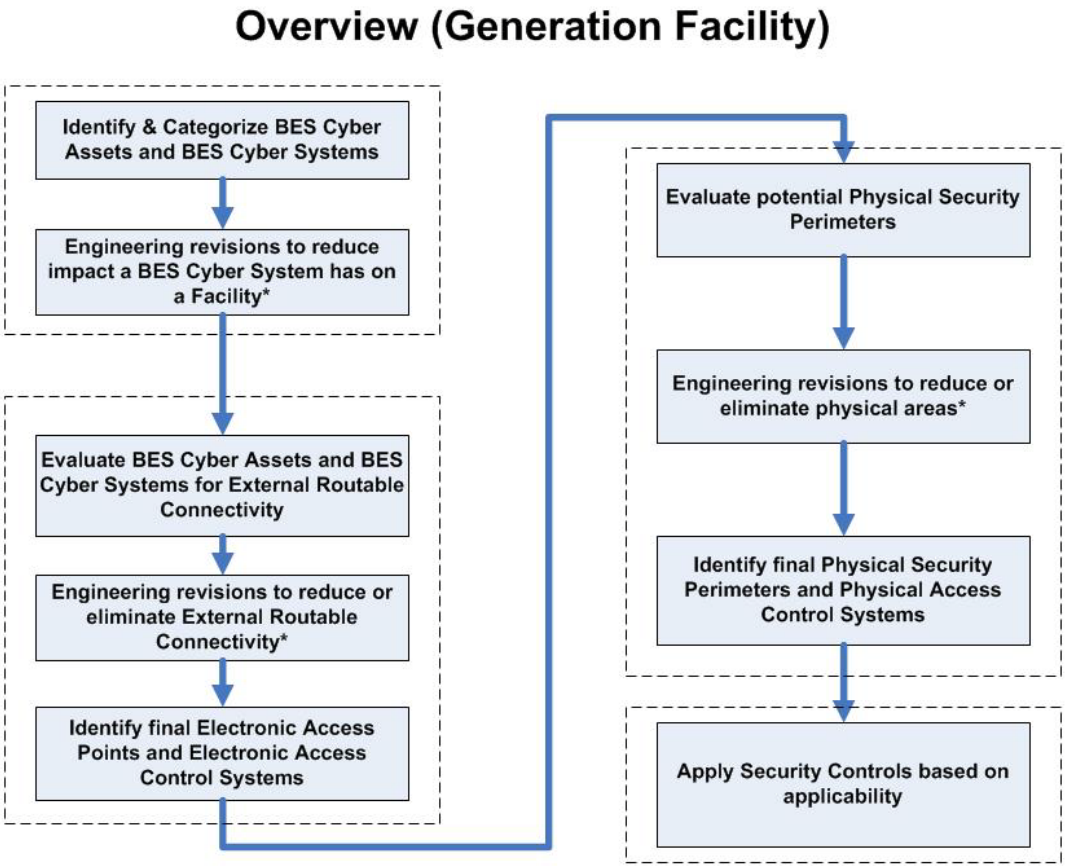
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3.	Update

		Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

4.1. Title: Cyber Security — CriticalBES Cyber Asset IdentificationSystem Categorization

5.2. Number: CIP-002-45

6. Purpose: NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

3. Purpose: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

7.4. Applicability:

4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

4.1. Reliability **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1. Balancing Authority

4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1. Each underfrequency load shedding (UFLS) or undervoltage load shedding (UVLS) system that:

4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3. Generator Operator

4.1.4. Generator Owner

~~**7.1.1. Interchange** **Coordinator.**~~

~~**7.1.2. Balancing Authority.**~~

~~**4.1.3**~~**4.1.5. or Interchange Authority**~~.~~

~~**7.1.3. Transmission Service Provider.**~~

4.1.6. Reliability Coordinator

~~**4.1.5**~~**4.1.7. Transmission** ~~Owner.~~**Operator**

~~**7.1.4. Transmission Operator.**~~

~~**4.1.7**~~**4.1.8.** ~~Generator~~ **Owner**~~.~~

~~**7.1.5. Generator Operator.**~~

~~**7.1.6. Load Serving Entity.**~~

~~**7.1.7. NERC.**~~

~~**7.1.8. Regional Entity.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.4.2.3. **Exemptions:** The following are exempt from Standard CIP-002-4:5:

4.2.14.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.34.2.3.3. In nuclear plants, theThe 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Date: The **Dates:**

1. **24 Months Minimum** – CIP-002-5 shall become effective on the later of July 1, 2015, or the first day of the eighth calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective approval.

5.2. In those jurisdictions where no regulatory approval is required CIP-002-5 shall become effective on the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

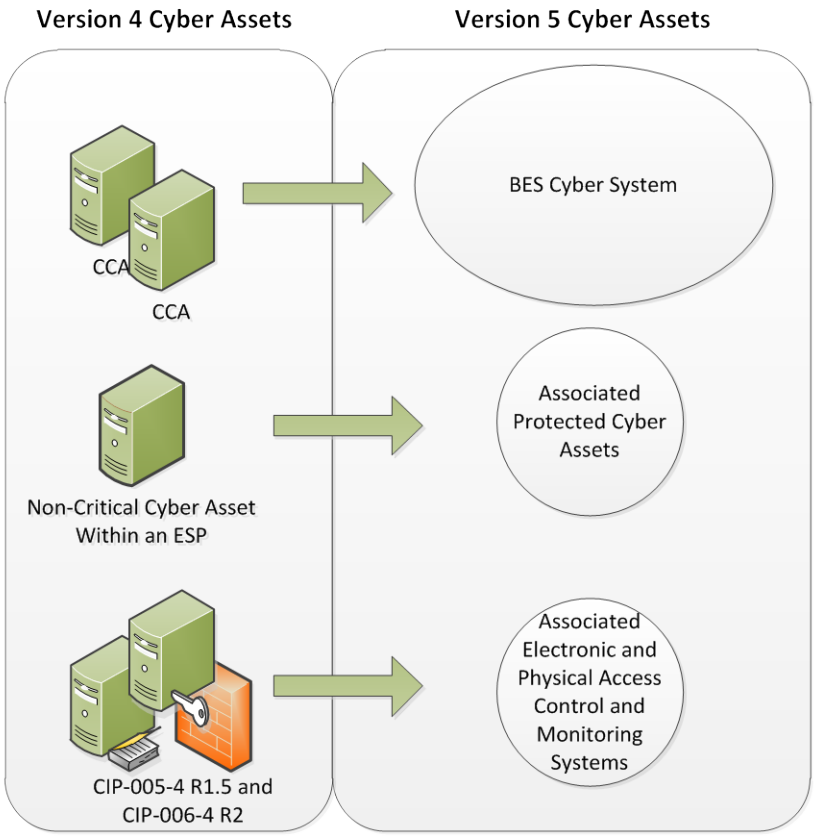
This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect the reliable operation of the Bulk Electric System. Several concepts provide the basis for the approach to the standard.

Throughout the standards, unless otherwise stated, bulleted items in the requirements are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section and the criteria in Attachment 1 of CIP-002 use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

BES Cyber Systems

One of the fundamental differences between Versions 4 and 5 of the CIP Cyber Security Standards is the shift from identifying Critical Cyber Assets to identifying BES Cyber Systems. This change results from the drafting team's review of the NIST Risk Management Framework and the use of an analogous term "information system" as the target for categorizing and applying security controls.



In transitioning from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets (as that term is used in Version 4). The CIP Cyber Security Standards use the "BES Cyber System" term primarily to provide a higher level for referencing the object of a requirement. For example, it becomes possible to apply requirements dealing with recovery and malware protection to a grouping rather than individual Cyber Assets, and it becomes clearer in the requirement that malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

Another reason for using the term "BES Cyber System" is to provide a convenient level at which a Responsible Entity can organize their documented implementation of the requirements and compliance evidence. Responsible Entities can use the well-developed concept of a *security plan* for each BES Cyber System to document the programs, processes, and plans in place to comply with security requirements.

It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System. For example, the Responsible Entity might choose to view an entire plant control system as a single BES Cyber System, or it might choose to view certain components of the plant control system as distinct BES Cyber Systems. The Responsible Entity should take into consideration the operational environment and

scope of management when defining the BES Cyber System boundary in order to maximize efficiency in secure operations. Defining the boundary too tightly may result in redundant paperwork and authorizations, while defining the boundary too broadly could make the secure operation of the BES Cyber System difficult to monitor and assess.

Reliable Operation of the BES

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Responsible Entities determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding functional entity's responsibilities as defined in its relationships with other functional entities in the NERC Functional Model. This ensures that the *initial* scope for consideration includes only those BES Cyber Systems and their associated BES Cyber Assets that perform or support the reliable operation of the BES. The definition of BES Cyber Asset provides the basis for this scoping.

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

Categorization Criteria

The criteria defined in Attachment 1 are used to categorize BES Cyber Systems into impact categories. Requirement 1 only requires the discrete identification of BES Cyber Systems for those in the high impact and medium impact categories. All BES Cyber Systems for Facilities not included in Attachment 1 – Impact Rating Criteria, Criteria 1.1 to 1.4 and Criteria 2.1 to 2.11 default to be low impact.

This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards.

Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets that are associated with BES Cyber Systems

BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems). These Cyber Assets include:

Electronic Access Control or Monitoring Systems ("EACMS") – Examples include: Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems.

Physical Access Control Systems ("PACS")– Examples include: authentication servers, card systems, and badge control systems.

Protected Cyber Assets ("PCA") – Examples may include, to the extent they are within the ESP: file servers, ftp servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems.

B. Requirements and Measures

R1. ~~Critical Asset Identification — The~~ Each Responsible Entity shall ~~develop a list of its identified Critical Assets determined~~implement a process that considers each of the following assets for purposes of parts 1.1 through ~~an annual application~~1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

i. Control Centers and backup Control Centers;
ii. Transmission stations and substations;
iii. Generation resources;
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
v. Special Protection Systems that support the reliable operation of the ~~criteria contained~~Bulk Electric System; and
vi. For Distribution Providers, Protection Systems specified in ~~*CIP-002* Applicability~~ section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1~~ — *Critical Asset Criteria*.~~, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

R2. The Responsible Entity shall: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Review the identifications in Requirement R1 and its parts (and update this list as necessary, and review it them if there are changes identified) at least annually.once every 15 calendar months, even if it has no identified items in Requirement R1, and

Critical Cyber Asset Identification — Using**2.2** Have its CIP Senior Manager or delegate approve the list of Critical Assets developed pursuant toidentifications required by Requirement R1, at least once every 15 calendar months, even if it has no identified items in Requirement R1.

M2. Acceptable evidence includes, but is not limited to, electronic or physical dated records to demonstrate that the Responsible Entity has reviewed and updated, where necessary, the identifications required in Requirement R1 and its parts, and has had its CIP Senior Manager or delegate approve the identifications required in Requirement R1 and its parts at least once every 15 calendar months, even if it has none identified in Requirement R1 and its parts, as required by Requirement R2.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall update this list as necessary, and review it at least annually.keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- ~~For~~ Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

CIP-002-5 - Attachment 1

Impact Rating Criteria

The criteria defined in Attachment 1 do not constitute stand-alone compliance requirements, but are criteria characterizing the level of impact and are referenced by requirements.

1. High Impact Rating (H)

Each BES Cyber System used by and located at any of the following:

1.1. Each Control Center or backup Control Center used to perform the functional obligations of the Reliability Coordinator.

1.2. Each Control Center or backup Control Center used to perform the functional obligations of the Balancing Authority: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9.

1.3. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2.4, 2.5, 2.7, 2.8, 2.9, or 2.10.

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the Generator Operator for one or more of the assets that meet criterion 2.1, 2.3, 2.6, or 2.9.

2. Medium Impact Rating (M)

Each BES Cyber System, not included in Section 1 above, associated with any of the following:

2.1. Commissioned generation, by each group of generating units ~~(including nuclear generation) at~~ at a single plant location ~~identified in Attachment 1, criterion 1.1~~, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber ~~Assets~~Systems that ~~must be considered~~meet this criterion are those shared BES Cyber ~~Assets~~Systems 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.~~ 1500 MW in a single Interconnection.

~~For the purpose of Standard CIP-002-4, Critical Cyber Assets are 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.~~

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.)

C. Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its records of approvals as specified in Requirement R3.

D. Compliance

9. Compliance Monitoring Process

4.1. Compliance Enforcement Authority

9.1.1. The Regional Entity shall serve as the Compliance Enforcement Authority with the following exceptions:

- For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.
- For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.
- 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.
- For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

4.2. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

4.3. Data Retention

9.3.1. The Responsible Entity shall keep documentation required by Standard CIP-002-4 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.

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

~~**4.4. Additional Compliance Information**~~

~~**9.4.1.** None.~~

~~**10. Violation Severity Levels**~~

2.2. Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities). The only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of resources that in aggregate equal or exceed 1000 MVAR.

2.3. Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year.

2.4. Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1~~	~~HIGH~~	~~N/A~~	~~N/A~~	~~The Responsible Entity has developed a list of Critical Assets but the list has not been reviewed and updated annually as required.~~	~~The Responsible Entity did not develop a list of its identified Critical Assets even if such list is null.~~
~~R2~~	~~HIGH~~	~~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.~~**Voltage Value of a Line**	~~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 Asset List.**Weight Value per Line**
R3	LOWER	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.)less than 200 kV (not applicable)	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.)(not applicable)
200 kV to 299 kV					700
300 kV to 499 kV					1300
500 kV and above					0

E. Regional Variances

None identified.

Version History

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	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. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	
4	4/19/12	FERC Order issued approving CIP-002-4 (approval becomes effective June 25, 2012) Added approved VRF/VSL table to section D.2.	

CIP-002-4 - Attachment 1

Critical Asset Criteria

The following are considered Critical Assets:

Each group of generating units (including nuclear generation)

1.1. Generation at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVAR or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates and informs the Generator Owner or Generator Operator as necessary to avoid BES Adverse Reliability Impacts in the long-term planning horizon.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first interconnection point of the generation unit(s) to be started, or up to the point on the Cranking Path where two or more path options exist, as identified in the Transmission Operator's restoration plan.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations or substations interconnected at 300 kV or higher with three or more other transmission stations or substations.

1.8.2.6. Transmission Facilities at a single station or substation location that are identified by theits Reliability Coordinator, Planning Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

1.9. Flexible AC Transmission Systems (FACTS), at a single station or substation location, that are identified by the Reliability Coordinator, Planning Authority or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

2.7. Transmission FacilitiesTransmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.10.2.8. Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the transmission system Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assetsgeneration

Facilities identified by any Generator Owner as a result of its application of Attachment 1, criterion 2.1.1 or 2.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12.2.9. Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching systemSystem that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more Interconnection Reliability Operating Limits (IROLs) violations for failure to operate as designed. or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable.

1.13.2.10. Each system or Facility group of Elements that performs automatic loadLoad shedding under a common control system, without human operator initiation, of 300 MW or more implementing Under Voltage Load Shedding undervoltage load shedding (UVLS) or Under Frequency Load Shedding underfrequency load shedding (UFLS) as required by the regional under a load shedding program that is subject to one or more requirements in a NERC or regional reliability standard.

1.14. Each control centerControl Center or backup control centerControl Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Reliability Coordinator.

1.15.2.11. Each control center or backup control center used to control generation at multiple plant locations, Generator Operator for any generation Facility or group of generation Facilities identified in criteria 1.1, 1.3, or 1.4. Each control center or backup control center used to control generationan aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection.

1.16. Each control centerControl Center or backup control centerControl Center used to perform the functional obligations of the Transmission Operator that includes control of at least one asset identified in criteria 1.2, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11 or 1.12.

2.12. Each control center or backup control center used to perform the functional obligations of the Balancing Authority that includes at least one asset identifiednot included in criteria 1.1, 1.3, 1.4, or 1.13. High Impact Rating (H), above.

1.17.2.13. Each control centerControl Center or backup control centerControl Center, not already included in High Impact Rating (H) above, used to perform the functional obligations of the Balancing Authority for generation equal to or greater than an aggregate of 1500 MW in a single Interconnection.

3. Low Impact Rating (L)

BES Cyber Systems not included in Sections 1 or 2 above that are associated with any of the following assets and that meet the applicability qualifications in Section 4 - Applicability, part 4.2 – Facilities, of this standard:

3.1. Control Centers and backup Control Centers.

3.2. Transmission stations and substations.

3.3. Generation resources.

3.4. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements.

3.5. Special Protection Systems that support the reliable operation of the Bulk Electric System.

3.6. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the qualified set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards. This section is especially significant in CIP-002-5 and represents the total scope of Facilities, systems, and equipment to which the criteria in Attachment 1 apply. This is important because it determines the balance of these Facilities, systems, and equipment that are Low Impact once those that qualify under the High and Medium Impact categories are filtered out.

For the purpose of identifying groups of Facilities, systems, and equipment, whether by location or otherwise, the Responsible Entity identifies assets as described in Requirement R1 of CIP-002-5. This is a process familiar to Responsible Entities that have to comply with versions 1, 2, 3, and 4 of the CIP standards for Critical Assets. As in versions 1, 2, 3, and 4, Responsible Entities may use substations, generation plants, and Control Centers at single site locations as identifiers of these groups of Facilities, systems, and equipment.

CIP-002-5

CIP-002-5 requires that applicable Responsible Entities categorize their BES Cyber Systems and associated BES Cyber Assets according to the criteria in Attachment 1. A BES Cyber Asset includes in its definition, "…that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact the reliable operation of the BES."

The following provides guidance that a Responsible Entity may use to identify the BES Cyber Systems that would be in scope. The concept of BES reliability operating service is useful in providing Responsible Entities with the option of a defined process for scoping those BES Cyber

Systems that would be subject to CIP-002-5. The concept includes a number of named BES reliability operating services. These named services include:

Dynamic Response to BES conditions
Balancing Load and Generation
Controlling Frequency (Real Power)
Controlling Voltage (Reactive Power)
Managing Constraints
Monitoring & Control
Restoration of BES
Situational Awareness
Inter-Entity Real-Time Coordination and Communication

Responsibility for the reliable operation of the BES is spread across all Entity Registrations. Each entity registration has its own special contribution to reliable operations and the following discussion helps identify which entity registration, in the context of those functional entities to which these CIP standards apply, performs which reliability operating service, as a process to identify BES Cyber Systems that would be in scope. The following provides guidance for Responsible Entities to determine applicable reliability operations services according to their Function Registration type.

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load & Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

Dynamic Response

The Dynamic Response Operating Service includes those actions performed by BES Elements or subsystems which are automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition. The types of dynamic responses that may be considered as potentially having an impact on the BES are:

- Spinning reserves (contingency reserves)
  - Providing actual reserve generation when called upon (GO,GOP)
  - Monitoring that reserves are sufficient (BA)
- Governor Response
  - Control system used to actuate governor response (GO)
- Protection Systems (transmission & generation)
  - Lines, buses, transformers, generators (DP, TO, TOP, GO, GOP)
  - Zone protection for breaker failure (DP, TO, TOP)
  - Breaker protection (DP, TO, TOP)
  - Current, frequency, speed, phase (TO,TOP, GO,GOP)
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays, and breakers, possibly software (DP, TO, TOP)
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers (DP)
- Power System Stabilizers (GO)

Balancing Load and Generation

The Balancing Load and Generation Operations Service includes activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time. Aspects of the Balancing Load and Generation function include, but are not limited to:

- Calculation of Area Control Error (ACE)
  - Field data sources (real time tie flows, frequency sources, time error, etc) (TO, TOP)
  - Software used to perform calculation (BA)
- Demand Response
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP,DP)
- Manually Initiated Load shedding
  - Ability to identify load change need (BA)
  - Ability to implement load changes (TOP, DP)

- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time (GO, BA)
  - Start units and provide energy (GOP)

Controlling Frequency (Real Power)

The Controlling Frequency Operations Service includes activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Frequency function include, but are limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics (BA, GOP, GO)
  - Software to calculate unit adjustments (BA)
  - Transmit adjustments to individual units (GOP)
  - Unit controls implementing adjustments (GOP)
- Regulation (regulating reserves)
  - Frequency source, schedule (BA)
  - Governor control system (GO)

Controlling Voltage (Reactive Power)

The Controlling Voltage Operations Service includes activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES. Aspects of the Controlling Voltage function include, but are not limited to:

- Automatic Voltage Regulation (AVR)
  - Sensors, stator control system, feedback (GO)
- Capacitive resources
  - Status, control (manual or auto), feedback (TOP, TO,DP)
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback (TOP,TO,DP)
- Static VAR Compensators (SVC)
  - Status, computations, control (manual or auto), feedback (TOP, TO,DP)

Managing Constraints

Managing Constraints includes activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES. Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC) (TOP)
- Interchange schedules (TOP, RC)
- Generation re-dispatch and unit commit (GOP)
- Identify and monitor SOL's & IROL's (TOP, RC)
- Identify and monitor Flow gates (TOP, RC)

Monitoring and Control

Monitoring and Control includes those activities, actions and conditions that provide monitoring and control of BES Elements. An example aspect of the Control and Operation function is:

- All methods of operating breakers and switches
  - SCADA (TOP, GOP)
  - Substation automation (TOP)

Restoration of BES

The Restoration of BES Operations Service includes activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance. Aspects of the Restoration of BES function include, but are not limited to:

- Restoration including planned cranking path
  - Through black start units (TOP, GOP)
  - Through tie lines (TOP, GOP)
- Off-site power for nuclear facilities. (TOP, TO, BA, RC, DP, GO, GOP)
- Coordination (TOP, TO, BA, RC, DP, GO, GOP)

Situational Awareness

The Situational Awareness function includes activities, actions and conditions established by policy, directive or standard operating procedure necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions. Aspects of the Situation Awareness function include:

- Monitoring and alerting (such as EMS alarms) (TOP, GOP, RC,BA)
- Change management (TOP,GOP,RC,BA)
- Current Day and Next Day planning (TOP)
- Contingency Analysis (RC)
- Frequency monitoring (BA, RC)

Inter-Entity Coordination

The Inter-Entity coordination and communication function includes activities, actions, and conditions established by policy, directive, or standard operating procedure necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES. Aspects of the Inter-Entity Coordination and Communication function include:

- Scheduled interchange (BA,TOP,GOP,RC)
- Facility operational data and status (TO, TOP, GO, GOP, RC, BA)
- Operational directives (TOP, RC, BA)

Applicability to Distribution Providers

It is expected that only Distribution Providers that own or operate facilities that qualify in the Applicability section will be subject to these Version 5 Cyber Security Standards. Distribution Providers that do not own or operate any facility that qualifies are not subject to these standards. The qualifications are based on the requirements for registration as a Distribution Provider and on the requirements applicable to Distribution Providers in NERC Standard EOP-005.

Requirement R1:

Requirement R1 implements the methodology for the categorization of BES Cyber Systems according to their impact on the BES. Using the traditional risk assessment equation, it reduces the measure of the risk to an impact (consequence) assessment, assuming the vulnerability index of 1 (the Systems are assumed to be vulnerable) and a probability of threat of 1 (100 percent). The criteria in Attachment 1 provide a measure of the impact of the BES assets supported by these BES Cyber Systems.

Responsible Entities are required to identify and categorize those BES Cyber Systems that have high and medium impact. BES Cyber Systems for BES assets not specified in Attachment 1, Criteria 1.1 – 1.4 and Criteria 2.1 – 2.11 default to low impact.

Attachment 1

Overall Application

In the application of the criteria in Attachment 1, Responsible Entities should note that the approach used is based on the impact of the BES Cyber System as measured by the bright-line criteria defined in Attachment 1.

- When the drafting team uses the term "Facilities", there is some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases, the criteria refer to a group of Facilities in a given location that supports the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to consider only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that supports reliable operation of the BES, as the Facilities that are subject to the criteria for categorization of BES Cyber Systems. Generation Facilities are separately discussed in the Generation section below. In CIP-002-5, these groups of Facilities, systems, and equipment are sometimes designated as BES assets. For example, an identified BES asset may be a named substation, generating plant, or Control Center. Responsible Entities have flexibility in how they group Facilities, systems, and equipment at a location.
- In certain cases, a BES Cyber System may be categorized by meeting multiple criteria. In such cases, the Responsible Entity may choose to document all criteria that result in the categorization. This will avoid inadvertent miscategorization when it no longer meets one of the criteria, but still meets another.
- It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

High Impact Rating (H)

This category includes those BES Cyber Systems, used by and at Control Centers (and the associated data centers included in the definition of Control Centers), that perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP), or Generator Operator (GOP), as defined under the Tasks heading of the applicable Function and the Relationship with Other Entities heading of the functional entity in the NERC Functional Model, and as scoped by the qualification in Attachment 1, Criteria 1.1, 1.2, 1.3 and 1.4. While those entities that have been registered as the above-named functional entities are specifically referenced, it must be noted that there may be agreements where some

of the functional obligations of a Transmission Operator may be delegated to a Transmission Owner (TO). In these cases, BES Cyber Systems at these TO Control Centers that perform these functional obligations would be subject to categorization as high impact. The criteria notably specifically emphasize functional obligations, not necessarily the RC, BA, TOP, or GOP facilities. One must note that the definition of Control Center specifically refers to reliability tasks for RCs, BAs, TOPs, and GOPs. A TO BES Cyber System in a TO facility that does not perform or does not have an agreement with a TOP to perform any of these functional tasks does not meet the definition of a Control Center. However, if that BES Cyber System operates any of the facilities that meet criteria in the Medium Impact category, that BES Cyber System would be categorized as a Medium Impact BES Cyber System.

The 3000 MW threshold defined in criterion 1.2 for BA Control Centers provides a sufficient differentiation of the threshold defined for Medium Impact BA Control Centers. An analysis of BA footprints shows that the majority of BAs with significant impact are covered under this criterion.

Additional thresholds as specified in the criteria apply for this category.

Medium Impact Rating (M)

Generation

The criteria in Attachment 1's medium impact category that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are criteria 2.1, 2.3, 2.6, 2.9, and 2.11. Criterion 2.13 for BA Control Centers is also included here.

- Criterion 2.1 designates as medium impact those BES Cyber Systems that impact generation with a net Real Power capability exceeding 1500 MW. The 1500 MW criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002, whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance." In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements as proposed by NERC standard MOD-024 and current development efforts in that area.

  By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected.

The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In Criterion 2.3, the drafting team sought to ensure that BES Cyber Systems for those generation Facilities that have been designated by the Planning Coordinator or Transmission Planner as necessary to avoid BES Adverse Reliability Impacts in the planning horizon of one year or more are categorized as medium impact. In specifying a planning horizon of one year or more, the intent is to ensure that those are units that are identified as a result of a "long term" reliability planning, i.e that the plans are spanning an operating period of at least 12 months: it does not mean that the operating day for the unit is necessarily beyond one year, but that the period that is being planned for is more than 1 year: it is specifically intended to avoid designating generation that is required to be run to remediate short term emergency reliability issues. These Facilities may be designated as "Reliability Must Run," and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, the focus on preventing an Adverse Reliability Impact dictates that these units are designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

  If it is determined through System studies that a unit must run in order to preserve the reliability of the BES, such as due to a Category C3 contingency as defined in TPL-003, then BES Cyber Systems for that unit are categorized as medium impact.

  The TPL standards require that, where the studies and plans indicate additional actions, that these studies and plans be communicated by the Planning Coordinator or Transmission Planner in writing to the Regional Entity/RRO. Actions necessary for the implementation of these plans by affected parties (generation owners/operators and Reliability Coordinators or other necessary party) are usually formalized in the form of an agreement and/or contract.

- Criterion 2.6 includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

  IROLs may be based on dynamic System phenomena such as instability or voltage collapse. Derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response.

- Criterion 2.9 categorizes BES Cyber Systems for Special Protection Systems and Remedial Action Schemes as medium impact. Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for. Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact.

- Criterion 2.11 categorizes as medium impact BES Cyber Systems used by and at Control Centers that perform the functional obligations of the Generator Operator for an aggregate generation of 1500 MW or higher in a single interconnection, and that have not already been included in Part 1. .

- Criterion 2.13 categorizes as medium impact those BA Control Centers that "control" 1500 MW of generation or more in a single interconnection and that have not already been included in Part 1. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Transmission

The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

- Criteria 2.2, 2.4 through 2.10, and 2.12 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a System to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). Criterion 2.2 includes BES Cyber Systems for those Facilities in Transmission Systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- Criterion 2.4 includes BES Cyber Systems for any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the

backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion in the medium impact category.

It must be noted that if the collector bus for a generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation in Criterion 2.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility, and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface." This collector bus would not be a facility for a medium impact BES Cyber System because it does not significantly affect the 500kV Transmission grid; it only affects a plant which is below the generation threshold.

- Criterion 2.5 includes BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion if they are deemed highly likely to have significant impact on the BES. While the criterion has been specified as part of the rationale for requiring protection for significant impact on the BES, the drafting team included, in this criterion, additional qualifications that would ensure the required level of impact to the BES. The drafting team:

  - Excluded radial facilities that would only provide support for single generation facilities.
  - Specified interconnection to at least three transmission stations or substations to ensure that the level of impact would be appropriate.

  The total aggregated weighted value of 3,000 was derived from weighted values related to three connected 345 kV lines and five connected 230 kV lines at a transmission station or substation. The total aggregated weighted value is used to account for the true impact to the BES, irrespective of line kV rating and mix of multiple kV rated lines.

  Additionally, in NERC's document "Integrated Risk Assessment Approach – Refinement to Severity Risk Index", Attachment 1, the report used an average MVA line loading based on kV rating:

  - 230 kV –> 700 MVA
  - 345 kV –> 1,300 MVA
  - 500 kV –> 2,000 MVA
  - 765 kV –> 3,000 MVA

  In the terms of applicable lines and connecting "other Transmission stations or substations" determinations, the following should be considered:

  - For autotransformers in a station, Responsible Entities have flexibility in determining whether the groups of Facilities are considered a single substation or station location or multiple substations or stations. In most cases, Responsible Entities

would probably consider them as Facilities at a single substation or station unless geographically dispersed. In these cases of these transformers being within the "fence" of the substation or station, autotransformers may not count as separate connections to other stations. The use of common BES Cyber Systems may negate any rationale for any consideration otherwise. In the case of autotransformers that are geographically dispersed from a station location, the calculation would take into account the connections in and out of each station or substation location.

- Multiple-point (or multiple-tap) lines are considered to contribute a single weight value per line and affect the number of connections to other stations. Therefore, a single 230 kV multiple-point line between three Transmission stations or substations would contribute an aggregated weighted value of 700 and connect Transmission Facilities at a single station or substation to two other Transmission stations or substations.

- Multiple lines between two Transmission stations or substations are considered to contribute multiple weight values per line, but these multiple lines between the two stations only connect one station to one other station. Therefore, two 345 kV lines between two Transmission stations or substations would contribute an aggregated weighted value of 2600 and connect Transmission Facilities at a single station or substation to one other Transmission station or substation.

Criterion 2.5's qualification for Transmission Facilities at a Transmission station or substation is based on 2 distinct conditions.

1. The first condition is that Transmission Facilities at a single station or substation where that station or substation connect, at voltage levels of 200 kV or higher to three (3) other stations or substations, to three other stations or substations. This qualification is meant to ensure that connections that operate at voltages of 500 kV or higher are included in the count of connections to other stations or substations as well.
2. The second qualification is that the aggregate value of all lines entering or leaving the station or substation must exceed 3000. This qualification does not include the consideration of lines operating at lower than 200 kV, or 500 kV or higher, the latter already qualifying as medium impact under criterion 2.4. : there is no value to be assigned to lines at voltages of less than 200 kV or 500 kV or higher in the table of values for the contribution to the aggregate value of 3000.

The Transmission Facilities at the station or substation must meet both qualifications to be considered as qualified under criterion 2.5.

- Criterion 2.6 include BES Cyber Systems for those Transmission Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as

specified by FAC-014-2, **Establish and Communicate System Operating Limits**, R5.1.1 and R5.1.3.

- Criterion 2.7 is sourced from the NUC-001 NERC standard, Requirement R9.2.2, for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown." In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Criterion 2.8 designates as medium impact those BES Cyber Systems that impact Transmission Facilities necessary to directly support generation that meet the criteria in Criteria 2.1 (generation Facilities with output greater than 1500 MW) and 2.3 (generation Facilities generally designated as "must run" for wide area reliability in the planning horizon). The Responsible Entity can request a formal statement from the Generation owner as to the qualification of generation Facilities connected to their Transmission systems.

- Criterion 2.9 designates as medium impact those BES Cyber Systems for those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching Systems installed to ensure BES operation within IROLs. The degradation, compromise or unavailability of these BES Cyber Systems would result in exceeding IROLs if they fail to operate as designed. By the definition of IROL, the loss or compromise of any of these have Wide Area impacts.

- Criterion 2.10 designates as medium impact those BES Cyber Systems for Systems or Elements that perform automatic Load shedding, without human operator initiation, of 300 MW or more. The SDT spent considerable time discussing the wording of Criterion 2.10, and chose the term "Each" to represent that the criterion applied to a discrete System or Facility. In the drafting of this criterion, the drafting team sought to include only those Systems that did not require human operator initiation, and targeted in particular those underfrequency load shedding (UFLS) Facilities and systems and undervoltage load shedding (UVLS) systems and Elements that would be subject to a regional Load shedding requirement to prevent Adverse Reliability Impact. These include automated UFLS systems or UVLS systems that are capable of Load shedding 300 MW or more. It should be noted that those qualifying systems which require a human operator to arm the system, but once armed, trigger automatically, are still to be considered as not requiring human operator initiation and should be designated as medium impact. The 300 MW threshold has been defined as the aggregate of the highest MW Load value, as defined by the applicable regional Load Shedding standards, for the preceding 12 months to account for seasonal fluctuations.

  This particular threshold (300 MW) was provided in CIP, Version 1. The SDT believes that the threshold should be lower than the 1500MW generation requirement since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric

System and hence requires a lower threshold. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

In ERCOT, the Load acting as a Resource ("LaaR") Demand Response Program is not part of the regional load shedding program, but an ancillary services market. In general, similar demand response programs that are not part of the NERC or regional reliability Load shedding programs, but are offered as components of an ancillary services market do not qualify under this criterion.

The language used in section 4 for UVLS and UFLS and in criterion 2.10 of Attachment 1 is designed to be consistent with requirements set in the PRC standards for UFLS and UVLS.

- Criterion 2.12 categorizes as medium impact those BES Cyber Systems used by and at Control Centers and associated data centers performing the functional obligations of a Transmission Operator and that have not already been categorized as high impact.

- Criterion 2.13 categorizes as Medium Impact those BA Control Centers that "control" 1500 MW of generation or more in a single Interconnection. The 1500 MW threshold is consistent with the impact level and rationale specified for Criterion 2.1.

Low Impact Rating (L)

BES Cyber Systems not categorized in high impact or medium impact default to low impact. Note that low impact BES Cyber Systems do not require discrete identification.

Restoration Facilities

- Several discussions on the CIP Version 5 standards suggest entities owning Blackstart Resources and Cranking Paths might elect to remove those services to avoid higher compliance costs. For example, one Reliability Coordinator reported a 25% reduction of Blackstart Resources as a result of the Version 1 language, and there could be more entities that make this choice under Version 5.

  In response, the CIP Version 5 drafting team sought informal input from NERC's Operating and Planning Committees. The committees indicate there has already been a reduction in Blackstart Resources because of increased CIP compliance costs, environmental rules, and other risks; continued inclusion within Version 5 at a category that would very significantly increase compliance costs can result in further reduction of a vulnerable pool.

  The drafting team moved from the categorization of restoration assets such as Blackstart Resources and Cranking Paths as medium impact (as was the case in earlier drafts) to categorization of these assets as low impact as a result of these considerations. This will not relieve asset owners of all responsibilities, as would have been the case in CIP-002, Versions 1-4 (since only Cyber Assets with routable connectivity which are essential to

restoration assets are included in those versions). Under the low impact categorization, those assets will be protected in the areas of cyber security awareness, physical access control, and electronic access control, and they will have obligations regarding incident response. This represents a net gain to bulk power system reliability, however, since many of those assets do not meet criteria for inclusion under Versions 1-4.

Weighing the risks to overall BES reliability, the drafting team determined that this re-categorization represents the option that would be the least detrimental to restoration function and, thus, overall BES reliability. Removing Blackstart Resources and Cranking Paths from medium impact promotes overall reliability, as the likely alternative is fewer Blackstart Resources supporting timely restoration when needed.

BES Cyber Systems for generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan default to low impact. NERC Standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan, as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired.

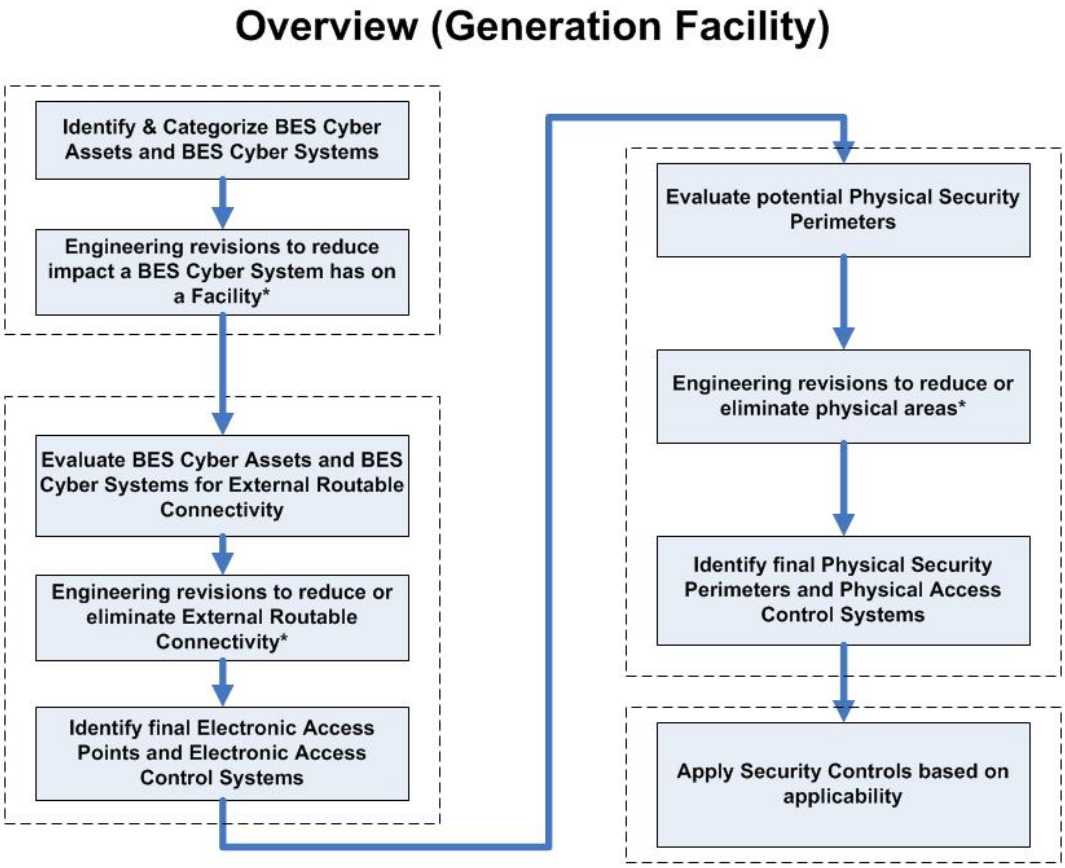
Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC Standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- BES Cyber Systems for Facilities and Elements comprising the Cranking Paths and meeting the initial switching requirements from the Blackstart Resource to the first Interconnection point of the generation unit(s) to be started, as identified in the Transmission Operator's restoration plan, default to the category of low impact: however, these systems are explicitly called out to ensure consideration for inclusion in the scope of the version 5 CIP standards. This requirement for inclusion in the scope is sourced from requirements in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started.

  Distribution Providers may note that they may have BES Cyber Systems that must be scoped in if they have Elements listed in the Transmission Operator's Restoration Plan that are components of the Cranking Path.

Use Case: CIP Process Flow

The following CIP use case process flow for a generator Operator/Owner was provided by a participant in the development of the Version 5 standards and is provided here as an example of a process used to identify and categorize BES Cyber Systems and BES Cyber Assets; review, develop, and implement strategies to mitigate overall risks; and apply applicable security controls.



* - Engineering revisions will need to be reviewed for cost justification, operational\safety requirements, support requirements, and technical limitations.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

BES Cyber Systems at each site location have varying impact on the reliable operation of the Bulk Electric System. Attachment 1 provides a set of "bright-line" criteria that the Responsible Entity must use to identify these BES Cyber Systems in accordance with the impact on the BES. BES Cyber Systems must be identified and categorized according to their impact so that the appropriate measures can be applied, commensurate with their impact. These impact categories will be the basis for the application of appropriate requirements in CIP-003-CIP-011.

Rationale for R2:

The lists required by Requirement R1 are reviewed on a periodic basis to ensure that all BES Cyber Systems required to be categorized have been properly identified and categorized. The miscategorization or non-categorization of a BES Cyber System can lead to the application of inadequate or non-existent cyber security controls that can lead to compromise or misuse that can affect the real-time operation of the BES. The CIP Senior Manager's approval ensures proper oversight of the process by the appropriate Responsible Entity personnel.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to	

		Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3. Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Security Management Controls

2. Number: CIP-003-5

3. Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-003-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

5. Effective Dates:

1. **24 Months Minimum** – CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects

are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

- **2.1** Cyber security awareness;
- **2.2** Physical security controls;
- **2.3** Electronic access controls for external routable protocol connections and Dial-up Connectivity; and
- **2.4** Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

R4. The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section “4. Applicability” of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section “4.1. Functional Entities” is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section “4.2. Facilities” defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term “Facilities” already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: ~~———~~Cyber Security — Security Management Controls~~__~~

2. Number: CIP-003-~~4~~5

3. Purpose: ~~Standard CIP-003-4 requires that Responsible Entities have minimum~~To specify consistent and sustainable security management controls ~~in place~~that establish responsibility and accountability to protect ~~Critical~~BES 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~~Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

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

4.1. ~~Reliability~~ **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~**4.1.1 Interchange** **Coordinator.**~~

~~**4.1.2 Balancing Authority.**~~

~~**4.1.3**~~**4.1.5 or Interchange Authority.**~~**

~~**4.1.4 Transmission Service Provider.**~~

4.1.6 Reliability Coordinator

~~**4.1.5**~~**4.1.7 Transmission** ~~Owner.~~**Operator**

~~**4.1.6 Transmission** Operator.~~

~~**4.1.7**~~**4.1.8** ~~Generator~~ **Owner.**~~**

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10** NERC.~~

~~**4.1.11** Regional Entity.~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.4.2.3 Exemptions: The following are exempt from Standard CIP-003-4:5:

4.2.14.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.34.2.3.3 In nuclear plants, theThe 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.

4.2.3.4 Responsible Entities For Distribution Providers, the systems and equipment that, are not included in compliance with Standard CIP-002 section 4, identify that they have no Critical Cyber Assets shall only be required to comply with .2.1 above.

5. Effective Dates:

4.2.41. **24 Months Minimum** – CIP-003-45, except for CIP-003-5, Requirement R2., shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval.

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).

2. In those jurisdictions where no regulatory approval is required, CIP-003-5, except for CIP-003-5, Requirement R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5, Requirement R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-003-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-

1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures provide examples of evidence to show documentation and implementation of the requirement. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

B. Requirements and Measures

~~Cyber Security Policy — The Responsible Entity shall~~

R1. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Personnel & training (CIP-004);

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.3 Physical security of BES Cyber Systems (CIP-006);

1.4 System security management (CIP-007);

1.5 Incident reporting and response planning (CIP-008);

1.6 Recovery plans for BES Cyber Systems (CIP-009);

1.7 Configuration change management and vulnerability assessments (CIP-010);

1.8 Information protection (CIP-011); and

1.9 Declaring and responding to CIP Exceptional Circumstances.

~~**R1.**~~ **M1.** Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a 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:~~

~~**1.1** The~~ management system that indicate review of each cyber security policy ~~addresses the requirements in Standards CIP-002-4 through CIP-009-4, including provision for emergency situations.~~

~~**R1.2.** The~~ at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy ~~is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets~~.

~~**1.2** Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.~~

~~Leadership —~~ **R2.** Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

2.1 Cyber security awareness;

2.2 Physical security controls;

2.3 Electronic access controls for external routable protocol connections and Dial-up Connectivity; and

2.4 Incident response to a Cyber Security Incident.

An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

M2. Examples of evidence may include, but are not limited to, one or more documented cyber security policies and evidence of processes, procedures, or plans that demonstrate the implementation of the required topics; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

~~**R2.**~~ **R4.** The Responsible Entity shall ~~assign a single senior manager with overall responsibility and~~ implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority ~~for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-4 through CIP-009-4.~~

~~**1.1** The senior manager shall be identified by name, title, and date of designation.~~

~~**1.2** Changes to the senior manager must be documented within thirty calendar days of the effective date.~~

~~**1.3**~~ , unless no delegations are used. Where allowed by the CIP Standards ~~CIP-002-4 through~~, the CIP ~~-009-4, the senior manager~~ Senior Manager may delegate authority for specific actions to a ~~named~~ delegate or delegates. These delegations shall be documented ~~in~~, including the ~~same manner as R2.1 and R2.2, and approved by the senior manager.~~

~~**1.4** The senior manager~~name or ~~delegate(s), shall authorize and document any exception from the requirements~~title 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~~, the specific actions delegated, and the date of the

delegation; approved by the ~~senior manager or delegate(s).~~ CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

~~**1.1** Documented exceptions to the cyber security policy must~~**M4.** An example of evidence may include ~~an explanation as to why the exception~~, but is ~~necessary and any compensating measures.~~

~~**1.2** Authorized exceptions to the cyber security policy must be reviewed and~~not limited to, a dated document, 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.~~

~~**1.1** 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~~CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve 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.~~

~~**1.2** 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~~authorize specifically identified ~~during the assessment.~~items.

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

~~**1.1** The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.~~

~~**5.1.1.** Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.~~

~~**5.1.2.** The list of personnel responsible for authorizing access to protected information shall be verified at least annually.~~

~~**1.2** 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.~~

~~**1.3** 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.~~C. 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~~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,~~ (“CEA”) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. ~~For the ERO, a third-party monitor without vested interest~~**Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in ~~the outcome~~this standard for ~~the ERO~~three calendar years.

~~**1.2.4**~~• If a Responsible Entity is found non-compliant, it shall ~~serve as~~keep information related to the non-compliance until mitigation is complete and approved or for the ~~Compliance Enforcement Authority~~time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Enforcement~~Assessment Processes~~:~~

- Compliance ~~Audits~~Audit
- Self-~~Certifications~~Certification
- Spot Checking
- Compliance ~~Violation Investigations~~Investigation
- 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.~~

- Complaint

~~1.5.~~1.4. 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.~~

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
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 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.
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).

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.
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.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
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 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.

E.D. Regional Variances

None identified.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2.

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The number of policies and their specific language are guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization, or as components of specific programs. The cyber security policy must cover in sufficient detail the nine topical areas required by CIP-003-5, Requirement R1. The Responsible Entity has the flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R1. Implementation of the cyber security policy is not specifically included in CIP-003-5, Requirement R1 as it is envisioned that the implementation of this policy is evidenced through successful implementation of CIP-004 through CIP-011. However, Responsible Entities are encouraged not to limit the scope of their cyber security policies to only those requirements from CIP-004 through CIP-011, but rather to put together a holistic cyber security policy appropriate to its organization. The assessment through the Compliance Monitoring and Enforcement Program of policy items that extend beyond the scope of CIP-004 through CIP-011 should not be considered candidates for potential violations. The Responsible Entity should consider the following for each of the required topics in its cyber security policy:

1.1 Personnel & training (CIP-004)

- Organization position on acceptable background investigations
- Identification of possible disciplinary action for violating this policy
- Account management

1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access

- Organization stance on use of wireless networks
- Identification of acceptable authentication methods
- Identification of trusted and untrusted resources
- Monitoring and logging of ingress and egress at Electronic Access Points
- Maintaining up-to-date anti-malware software before initiating Interactive Remote Access
- Maintaining up-to-date patch levels for operating systems and applications used to initiate Interactive Remote Access
- Disabling VPN "split-tunneling" or "dual-homed" workstations before initiating Interactive Remote Access
- For vendors, contractors, or consultants: include language in contracts that requires adherence to the Responsible Entity's Interactive Remote Access controls

1.3 Physical security of BES Cyber Systems (CIP-006)

- Strategy for protecting Cyber Assets from unauthorized physical access
- Acceptable physical access control methods
- Monitoring and logging of physical ingress

1.4 System security management (CIP-007)

- Strategies for system hardening
- Acceptable methods of authentication and access control
- Password policies including length, complexity, enforcement, prevention of brute force attempts
- Monitoring and logging of BES Cyber Systems

1.5 Incident reporting and response planning (CIP-008)

- Recognition of Cyber Security Incidents
- Appropriate notifications upon discovery of an incident
- Obligations to report Cyber Security Incidents

1.6 Recovery plans for BES Cyber Systems (CIP-009)

- Availability of spare components

- Availability of system backups

1.7 Configuration change management and vulnerability assessments (CIP-010)

- Initiation of change requests
- Approval of changes
- Break-fix processes

1.8 Information protection (CIP-011)

- Information access control methods
- Notification of unauthorized information disclosure
- Information access on a need-to-know basis

1.9 Declaring and responding to CIP Exceptional Circumstances

- Processes to invoke special procedures in the event of a CIP Exceptional Circumstance
- Processes to allow for exceptions to policy that do not violate CIP requirements

The Standard Drafting Team (SDT) has removed requirements relating to exceptions to a Responsible Entity's security policies since it is a general management issue that is not within the scope of a reliability requirement. The SDT considers it to be an internal policy requirement and not a reliability requirement. However, the SDT encourages Responsible Entities to continue this practice as a component of its cyber security policy.

In this and all subsequent required approvals in the NERC CIP Standards, the Responsible Entity may elect to use hardcopy or electronic approvals to the extent that there is sufficient evidence to ensure the authenticity of the approving party.

Requirement R2:

As with Requirement R1, the number of policies and their specific language would be guided by a Responsible Entity's management structure and operating conditions. Policies might be included as part of a general information security program for the entire organization or as components of specific programs. The cyber security policy must cover in sufficient detail the four topical areas required by CIP-003-5, Requirement R2. The Responsible Entity has flexibility to develop a single comprehensive cyber security policy covering these topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail in lower level documents in its documentation hierarchy. In the case of a high-level umbrella policy, the Responsible Entity would be expected to provide the high-level policy as well as the additional documentation in order to demonstrate compliance with CIP-003-5, Requirement R2. The intent of the requirement is to outline a set of basic protections that all low impact BES Cyber Systems should receive without requiring a significant administrative and compliance overhead. The SDT intends that demonstration of this requirement can be reasonably accomplished through providing evidence of related processes, procedures, or plans. While the audit staff may choose to review an example low impact BES Cyber System, the SDT believes strongly that the current method (as of this writing) of reviewing a statistical sample of systems is not

necessary. The SDT also notes that in topic 2.3, the SDT uses the term "electronic access control" in the general sense, i.e., to control access, and not in the specific technical sense requiring authentication, authorization, and auditing.

Requirement R3:

The intent of CIP-003-5, Requirement R3 is effectively unchanged since prior versions of the standard. The specific description of the CIP Senior Manager has now been included as a defined term rather than clarified in the Standard itself to prevent any unnecessary cross-reference to this standard. It is expected that this CIP Senior Manager play a key role in ensuring proper strategic planning, executive/board-level awareness, and overall program governance.

Requirement R4:

As indicated in the rationale for CIP-003-5, Requirement R4, this requirement is intended to demonstrate a clear line of authority and ownership for security matters. The intent of the SDT was not to impose any particular organizational structure, but, rather, the Responsible Entity should have significant flexibility to adapt this requirement to their existing organizational structure. A Responsible Entity may satisfy this requirement through a single delegation document or through multiple delegation documents. The Responsible Entity can make use of the delegation of the delegation authority itself to increase the flexibility in how this applies to its organization. In such a case, delegations may exist in numerous documentation records as long as the collection of these documentation records provides a clear line of authority back to the CIP Senior Manager. In addition, the CIP Senior Manager could also choose not to delegate any authority and meet this requirement without such delegation documentation.

The Responsible Entity must keep its documentation of the CIP Senior Manager and any delegations up to date. This is to ensure that individuals do not assume any undocumented authority. However, delegations do not have to be re-instated if the individual who delegated the task changes roles or is replaced. For instance, assume that John Doe is named the CIP Senior Manager and he delegates a specific task to the Substation Maintenance Manager. If John Doe is replaced as the CIP Senior Manager, the CIP Senior Manager documentation must be updated within the specified timeframe, but the existing delegation to the Substation Maintenance Manager remains in effect as approved by the previous CIP Senior Manager, John Doe.

Rationale:

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT approval, the text from the rationale text boxes was moved to this section.

Rationale for R1:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

Annual review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R2:

One or more security policies enable effective implementation of the standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. The Responsible Entity can demonstrate through its policies that its management supports the accountability and responsibility necessary for effective implementation of the standard's requirements.

The language in Requirement R2, Part 2.3 ". . . for external routable protocol connections and Dial-up Connectivity . . ." was included to acknowledge the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact. Part 2.3 uses the phrase "external routable protocol connections" instead of the defined term "External Routable Connectivity," because the latter term has very specific connotations relating to Electronic Security Perimeters and high and medium impact BES Cyber Systems. Using the glossary term "External Routable Connectivity" in the context of Requirement R2 would not be appropriate because Requirement R2 is limited in scope to low impact BES Cyber Systems.

Review and approval of the cyber security policy at least every 15 calendar months ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems.

Rationale for R3:

The identification and documentation of the single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization, as called for in Blackout Report Recommendation 43. The language that identifies CIP Senior Manager responsibilities is included in the *Glossary of Terms used in NERC Reliability Standards* so that it may be used across the body of CIP standards without an explicit cross-reference.

FERC Order No. 706, Paragraph 296, requests consideration of whether the single senior manager should be a corporate officer or equivalent. As implicated through the defined term, the senior manager has "the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards" which ensures that the senior manager is of sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for responsible entities, from municipal, cooperative, federal agencies, investor owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a "corporate officer or equivalent" would be extremely difficult to interpret and enforce on a consistent basis.

Rationale for R4:

The intent of the requirement is to ensure clear accountability within an organization for certain security matters. It also ensures that delegations are kept up-to-date and that individuals do not assume undocumented authority.

In FERC Order No. 706, Paragraphs 379 and 381, the Commission notes that Recommendation 43 of the 2003 Blackout Report calls for "clear lines of authority and ownership for security matters." With this in mind, the Standard Drafting Team has sought to provide clarity in the requirement for delegations so that this line of authority is clear and apparent from the documented delegations.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. ~~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	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	~~Update~~
3	3/31/10	Approved by FERC.	
4	~~Board approved 01~~1/24/~~2011~~11	~~**Update version number from "3" to "4"**~~Approved by the NERC Board of Trustees.	Update to conform to changes to CIP-002-4 (Project 2008-06)
~~4~~5	~~4/19~~11/26/12	~~FERC Order issued approving CIP-003-4 (approval becomes effective June 25, 2012)~~ ~~**Added approved VRF/VSL table to section D.2.**~~Adopted by the NERC Board	Modified to coordinate with other CIP standards and to revise format to

		of Trustees.	use RBS Template.

A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-5

3. **Purpose:** To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

4.2. **Facilities:** For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-004-5:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3. 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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of

implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.

- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Page 6 of 52

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

Page 7 of 52

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Page 8 of 52

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

Page 9 of 52

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

Page 10 of 52

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

Page 11 of 52

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

Page 12 of 52

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

Page 13 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Page 14 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Page 15 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Page 16 of 52

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Page 17 of 52

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Page 18 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Page 19 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Page 20 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Page 21 of 52

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Page 22 of 52

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms and evidence, when dated, which can be used are:

- 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.).

Requirement R2:

Training shall cover the policies, access controls, and procedures as developed for the BES Cyber Systems and include, at a minimum, the required items appropriate to personnel roles and responsibilities from Table R2. The Responsible Entity has the flexibility to define the training program and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. Identity only needs to be confirmed prior to initially granting access and only requires periodic confirmation according to the entity's process during the tenure of employment, which may or may not be the same as the initial verification action.

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include

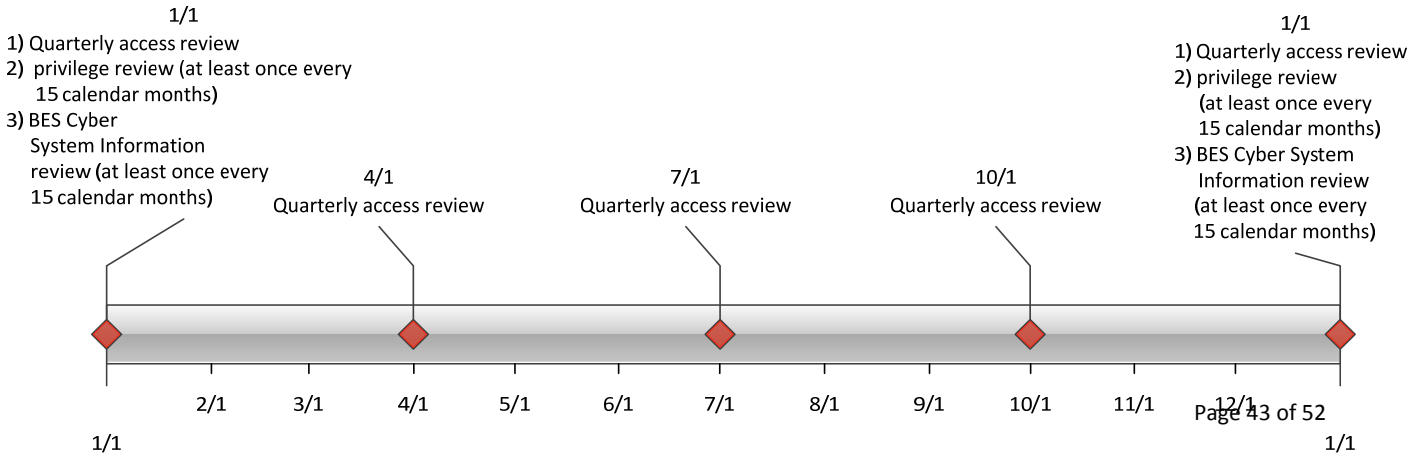
individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group



assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Scenario	Possible Process
Immediate involuntary termination	Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.
Scheduled involuntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Voluntary termination	Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
Retirement where the last working day is several weeks prior to the termination date	Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
Death	Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:
    - The visitor control program
    - Electronic interconnectivity supporting the operation and control of BES Cyber Systems
    - Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. “Authorization” should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. “Provisioning” should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity’s policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A.A. Introduction

1. **Title:** Cyber Security — Personnel & Training

2. **Number:** CIP-004-45

3. **Purpose:** Standard CIP-004-4 requiresTo minimize the risk against compromise that personnel having authorized cybercould lead to misoperation or authorized unescorted physical access to Criticalinstability in the BES from individuals accessing BES Cyber Assets, including contractors and service vendors, haveSystems by requiring an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part in support of a group of standards numbered Standards CIP-002-4 through CIP-009-4.protecting BES Cyber Systems.

4. **Applicability:**

   4.1. Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

   4.1. Reliability Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

4.1.4. Generator Owner

~~**4.1.1 Interchange** **Coordinator.**~~

~~**4.1.2 Balancing Authority.**~~

~~**4.1.3**~~**4.1.5. or Interchange Authority**~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6. Reliability Coordinator

~~**4.1.5**~~**4.1.7. Transmission** ~~Owner.~~**Operator**

~~**4.1.6 Transmission** Operator.~~

~~**4.1.7**~~**4.1.8.** ~~Generator~~ **Owner**~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.4.2.3. **Exemptions:** The following are exempt from Standard CIP-004-4:5:

4.2.14.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.34.2.3.3. ~~In nuclear plants, the~~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.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.44.2.3.5. Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical Cyber Assets.~~ BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ The Dates:

1. **24 Months Minimum** – CIP-004-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ~~eighth~~ninth calendar quarter after the effective date of the order providing 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~~ approval.

5.2. In those jurisdictions where no regulatory approval is ~~not~~ required~~)~~., CIP-004-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~4.1.2. **Requirements**~~

~~Awareness The~~ **6. Background:**

Standard CIP-004-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each 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~~ *one or more documented [processes, plan, etc] that include* ~~security awareness reinforcement on at least a quarterly~~*the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis ~~using~~for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R1 – Security Awareness Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R1 – Security Awareness Program

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	An example of evidence may include, but is not limited to, documentation that the quarterly reinforcement has been provided. Examples of evidence of reinforcement may include, but are not limited to, dated copies of information used to reinforce security awareness, as well as evidence of distribution, such as: • direct communications (for example, e-mails, memos, computer-based training); or • indirect communications (for example, posters, intranet, or brochures); or • management support and reinforcement (for example, presentations or meetings).

Page 6 of 62

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M2. Evidence must include the training program that includes each of the applicable requirement parts in *CIP-004-5 Table R2 – Cyber Security Training Program* and additional evidence to demonstrate implementation of the program(s).

Page 7 of 62

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Training content on: 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets.	Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.

Page 8 of 62

CIP-004-5 Table R2 – Cyber Security Training Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, training records and documentation of when CIP Exceptional Circumstances were invoked.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	Examples of evidence may include, but are not limited to, dated individual training records.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

Page 9 of 62

M3. Evidence must include the documented personnel risk assessment programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R3 – Personnel Risk Assessment Program* and additional evidence to demonstrate implementation of the program(s).

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to confirm identity.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to confirm identity.

Page 10 of 62

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes: 3.2.1. current residence, regardless of duration; and 3.2.2. other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to perform a seven year criminal history records check.

Page 11 of 62

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process to evaluate criminal history records checks for authorizing access.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process to evaluate criminal history records checks.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's criteria or process for verifying contractors or service vendors personnel risk assessments.

Page 12 of 62

CIP-004-5 Table R3 – Personnel Risk Assessment Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	An example of evidence may include, but is not limited to, documentation of the Responsible Entity's process for ensuring that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed within the last seven years.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access management programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Same Day Operations].*

M4. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-004-5 Table R4 – Access Management Program* and additional evidence to demonstrate that the access management program was implemented as described in the Measures column of the table.

Page 13 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter; and 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	An example of evidence may include, but is not limited to, dated documentation of the process to authorize electronic access, unescorted physical access in a Physical Security Perimeter, and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Page 14 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Examples of evidence may include, but are not limited to: • Dated documentation of the verification between the system generated list of individuals who have been authorized for access (i.e., workflow database) and a system generated list of personnel who have access (i.e., user account listing), or • Dated documentation of the verification between a list of individuals who have been authorized for access (i.e., authorization forms) and a list of individuals provisioned for access (i.e., provisioning forms or shared account listing).

Page 15 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	An example of evidence may include, but is not limited to, documentation of the review that includes all of the following: 1. A dated listing of all accounts/account groups or roles within the system; 2. A summary description of privileges associated with each group or role; 3. Accounts assigned to the group or role; and 4. Dated evidence showing verification of the privileges for the group are authorized and appropriate to the work function performed by people assigned to each account.

Page 16 of 62

CIP-004-5 Table R4 – Access Management Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	An example of evidence may include, but is not limited to, the documentation of the review that includes all of the following: 1. A dated listing of authorizations for BES Cyber System information; 2. Any privileges associated with the authorizations; and 3. Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions.

Page 17 of 62

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].*

M5. Evidence must include each of the applicable documented programs that collectively include each of the applicable requirement parts in *CIP-004-5 Table R5 – Access Revocation* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form verifying access removal associated with the termination action; and 2. Logs or other demonstration showing such persons no longer have access.

Page 18 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	An example of evidence may include, but is not limited to, documentation of all of the following: 1. Dated workflow or sign-off form showing a review of logical and physical access; and 2. Logs or other demonstration showing such persons no longer have access that the Responsible Entity determines is not necessary.

Page 19 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PACS	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form verifying access removal to designated physical areas or cyber systems containing BES Cyber System Information associated with the terminations and dated within the next calendar day of the termination action.

Page 20 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	An example of evidence may include, but is not limited to, workflow or sign-off form showing access removal for any individual BES Cyber Assets and software applications as determined necessary to completing the revocation of access and dated within thirty calendar days of the termination actions.

Page 21 of 62

CIP-004-5 Table R5 – Access Revocation			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: • EACMS	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Examples of evidence may include, but are not limited to: • Workflow or sign-off form showing password reset within 30 calendar days of the termination; • Workflow or sign-off form showing password reset within 30 calendar days of the reassignments or transfers; or • Documentation of the extenuating operating circumstance and workflow or sign-off form showing password reset within 10 calendar days following the end of the operating circumstance.

Page 22 of 62

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Lower	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	Operations Planning	Lower	The Responsible Entity implemented a cyber security training program but failed to include one of the training	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical	deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with authorized electronic or authorized unescorted physical	implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	(2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			date, and did not identify, assess and correct the deficiencies. (2.3)			
R3	Operations Planning	Medium	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies.	contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies.	for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7	(3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7	OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15	BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is	calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information storage locations, privileges

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)			were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented	complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar	Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identify, assess, and correct the deficiencies. (5.5)			

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The security awareness program is intended to be an informational program, not a formal training program. It should reinforce security practices to ensure that personnel maintain awareness of best practices for both physical and electronic security to protect its BES Cyber Systems. The Responsible Entity is not required to provide records that show that each individual received or understood the information, but they must maintain documentation of the program materials utilized in the form of posters, memos, and/or presentations.

Examples of possible mechanisms ~~such as~~and evidence, when dated, which can be used are:

- ~~R1.~~ Direct communications (e.g., emails, memos, computer based training, etc.);
- ~~R2.~~ Indirect communications (e.g., posters, intranet, brochures, etc.);

R3.• Management support and reinforcement (e.g., presentations, meetings, etc.).

- 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.

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.**Requirement R2:**

Training shall cover the policies, access controls, and procedures as developed for the CriticalBES Cyber Assets covered by CIP-004-4,Systems and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

- The proper use of Critical Cyber Assets;
- Physical and electronic access controls to Critical Cyber Assets;
- The proper handling of Critical Cyber Asset information; and,
- Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

from Table R2. The Responsible Entity shall maintain documentation that training is conducted at least annually, includinghas the dateflexibility to define the training was completed and attendance recordsprogram and it may consist of multiple modules and multiple delivery mechanisms, but a single training program for all individuals needing to be trained is acceptable. The training can focus on functions, roles or responsibilities at the discretion of the Responsible Entity.

Personnel Risk Assessment — The Responsible Entity shall have a documented personnel risk assessment program,One new element in the training content is intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems as per FERC Order No. 706, Paragraph 434. This is not intended to provide technical training to individuals supporting networking hardware and software, but educating system users of the cyber security risks associated with the interconnectedness of these systems. The users, based on their function, role or responsibility, should have a basic understanding of which systems can be accessed from other systems and how the actions they take can affect cyber security.

Each Responsible Entity shall ensure all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, complete cyber security training prior to their being granted authorized access, except for CIP Exceptional Circumstances. To retain the authorized accesses, individuals must complete the training at least one every 15 months.

Requirement R3:

- Each Responsible Entity shall ensure a personnel risk assessment is performed for all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems, including contractors and service vendors, prior to their being granted authorized access, except for program specified

exceptional circumstances that are approved by the single senior management official or their delegate and impact the reliability of the BES or emergency response. Identity should be confirmed 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~~. Identity only needs to be confirmed prior to initially granting access ~~except in specified circumstances such as an emergency.~~

~~The personnel risk assessment program shall at a minimum include:~~

~~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.~~

~~The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.~~

~~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.~~

- ~~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 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.~~

~~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.~~

~~4.1.3. Measures~~

~~The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.~~

~~The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.~~

~~The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.~~

~~The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.~~

4.1.29. **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 only requires periodic confirmation according to the Regional Entity,entity's process during the Regional Entity shall serve astenure of employment, which may or may not be the Compliance Enforcement Authoritysame as the initial verification action.

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 personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

1.4.2. The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 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.

~~**1.4.3.** 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**~~

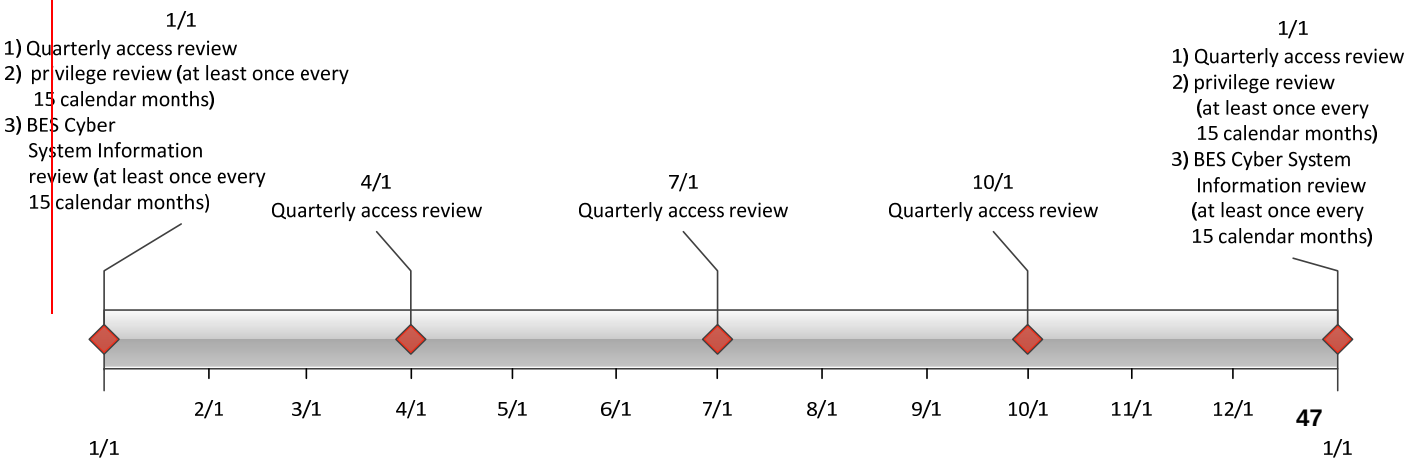
~~**2. Violation Severity Levels**~~

A seven year criminal history check should be performed for those locations where the individual has resided for at least six consecutive months. This check should also be performed in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. When it is not possible to perform a full seven year criminal history check, documentation must be made of what criminal history check was performed, and the reasons a full seven-year check could not be performed. Examples of this could include individuals under the age of 25 where a juvenile criminal history may be protected by law, individuals who may have resided in locations from where it is not possible to obtain a criminal history records check, violates the law or is not allowed under the existing collective bargaining agreement. The Responsible Entity should consider the absence of information for the full seven years when assessing the risk of granting access during the process to evaluate the criminal history check. There needs to be a personnel risk assessment that has been completed within the last seven years for each individual with access. A new criminal history records check must be performed as part of the new PRA. Individuals who have been granted access under a previous version of these standards need a new PRA within seven years of the date of their last PRA. The clarifications around the seven year criminal history check in this version do not require a new PRA be performed by the implementation date.

Requirement R4:

Authorization for electronic and unescorted physical access and access to BES Cyber System Information must be on the basis of necessity in the individual performing a work function. Documentation showing the authorization should have some justification of the business need included. To ensure proper segregation of duties, access authorization and provisioning should not be performed by the same person where possible.

This requirement specifies both quarterly reviews and reviews at least once every 15 calendar months. Quarterly reviews are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.



The privilege review at least once every 15 calendar months is more detailed to ensure an individual's associated privileges are the minimum necessary to perform their work function (i.e., least

privilege). Entities can more efficiently perform this review by implementing role-based access. This involves determining the specific roles on the system (e.g., system operator, technician, report viewer, administrator, etc.) then grouping access privileges to the role and assigning users to the role. Role-based access does not assume any specific software and can be implemented by defining specific provisioning processes for each role where access group assignments cannot be performed. Role-based access permissions eliminate the need to perform the privilege review on individual accounts. An example timeline of all the reviews in Requirement R4 is included below.

Separation of duties should be considered when performing the reviews in Requirement R4. The person reviewing should be different than the person provisioning access.

If the results of quarterly or at least once every 15 calendar months account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that this error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Requirement R5:

The requirement to revoke access at the time of the termination action includes procedures showing revocation of access concurrent with the termination action. This requirement recognizes that the timing of the termination action may vary depending on the circumstance. Some common scenarios and possible processes on when the termination action occurs are provided in the following table. These scenarios are not an exhaustive list of all scenarios, but are representative of several routine business practices.

Requirement	VRF	Lower VSL	Moderate VSL	High VSLScenario	Severe VSLPossible Process	
R1.	LOWER	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.
R2.	LOWER	The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.		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	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

					unescorted physical access to Critical Cyber Assets.	access to Critical Cyber Assets.
R2.1.	MEDIUM	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.Immediate involuntary termination	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.Human resources or corporate security escorts the individual off site and the supervisor or human resources personnel notify the appropriate personnel to begin the revocation process.	
R2.2.	MEDIUM	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.
R2.2.1.	LOWER	N/A			N/A	N/A	N/A
R2.2.2.	LOWER	N/A			N/A	N/A	N/A
R2.2.3.	LOWER	N/A			N/A	N/A	N/A
R2.2.4.	LOWER	N/A			N/A	N/A	N/A

R2.3.	LOWER	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.
R3.	MEDIUM	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 bargaining unit agreements, 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.Scheduled involuntary termination	The Responsible Entity does not 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. 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.Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.		
R3.1.	LOWER	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.
R3.2.	LOWER	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.
R3.3.	LOWER	The Responsible Entity did not document the results of	The Responsible Entity did not document the results of personnel risk	The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel	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-		

		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.	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.	with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. Voluntary termination	004-4. Human resources personnel are notified of the termination and work with appropriate personnel to schedule the revocation of access at the time of termination.
R4.	LOWER	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 at least one individual but less than 5% 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 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 but less than 15%of the authorized personnel. Retirement where the last working day is several weeks prior to the termination date	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 of the authorized personnel. Human resources personnel coordinate with manager to determine the final date access is no longer needed and schedule the revocation of access on the determined day.
R4.1.	LOWER	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. Death	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. Human resources personnel are notified of the death and work with appropriate personnel to begin the revocation process.

~~R4.2.~~	~~MEDIUM~~	~~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.~~

~~4.1.31. **Regional Variances**~~

~~None identified.~~

Revocation of electronic access should be understood to mean a process with the end result that electronic access to BES Cyber Systems is no longer possible using credentials assigned to or known by the individual(s) whose access privileges are being revoked. Steps taken to accomplish this outcome may include deletion or deactivation of accounts used by the individual(s), but no specific actions are prescribed. Entities should consider the ramifications of deleting an account may include incomplete event log entries due to an unrecognized account or system services using the account to log on.

The initial revocation required in Requirement R5.1 includes unescorted physical access and Interactive Remote Access. These two actions should prevent any further access by the individual after termination. If an individual still has local access accounts (i.e., accounts on the Cyber Asset itself) on BES Cyber Assets, then the Responsible Entity has 30 days to complete the revocation process for those accounts. However, nothing prevents a Responsible Entity from performing all of the access revocation at the time of termination.

For transferred or reassigned individuals, a review of access privileges should be performed. This review could entail a simple listing of all authorizations for an individual and working with the respective managers to determine which access will still be needed in the new position. For instances in which the individual still needs to retain access as part of a transitory period, the entity should schedule a time to review these access privileges or include the privileges in the quarterly account review or annual privilege review.

Revocation of access to shared accounts is called out separately to prevent the situation where passwords on substation and generation devices are constantly changed due to staff turnover.

Requirement 5.5 specified that passwords for shared account are to the changed within 30 calendar days of the termination action or when the Responsible Entity determines an individual no longer requires access to the account as a result of a reassignment or transfer. The 30 days applies under normal operating conditions. However, circumstances may occur where this is not possible. Some systems may require an outage or reboot of the system in order to complete the password change. In periods of extreme heat or cold, many Responsible Entities may prohibit system outages and reboots in order to maintain reliability of the BES. When these circumstances occur, the Responsible Entity must document these circumstances and prepare to change the password within 10 calendar days following the end of the operating circumstances. Records of activities must be retained to show that the Responsible Entity followed the plan they created.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Ensures that Responsible Entities with personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Assets take action so that those personnel with such authorized electronic or authorized unescorted physical access maintain awareness of the Responsible Entity's security practices.

Summary of Changes: Reformatted into table structure.

Reference to prior version: (Part 1.1) CIP-004-4, R1

Change Rationale: (Part 1.1)

Changed to remove the need to ensure or prove everyone with authorized electronic or authorized unescorted physical *access "received" ongoing reinforcement – to state that security awareness has been reinforced.*

Moved example mechanisms to guidance.

Rationale for R2:

To ensure that the Responsible Entity's training program for personnel who need authorized electronic access and/or authorized unescorted physical access to BES Cyber Systems covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.

Based on their role, some personnel may not require training on all topics.

Summary of Changes:

1. Addition of specific role training for:

- The visitor control program
- Electronic interconnectivity supporting the operation and control of BES Cyber Systems
- Storage media as part of the handling of BES Cyber Systems information

2. Change references from Critical Cyber Assets to BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP004-4, R2.2.1

Change Rationale: (Part 2.1)

Removed "proper use of Critical Cyber Assets" concept from previous versions to focus the requirement on cyber security issues, not the business function. The previous version was

focused more on the business or functional use of the BES Cyber System and is outside the scope of cyber security. Personnel who will administer the visitor control process or serve as escorts for visitors need training on the program. Core training on the handling of BES Cyber System (not Critical Cyber Assets) Information, with the addition of storage; FERC Order No. 706, paragraph 413 and paragraphs 632-634, 688, 732-734; DHS 2.4.16. Core training on the identification and reporting of a Cyber Security Incident; FERC Order No. 706, Paragraph 413; Related to CIP-008-5 & DHS Incident Reporting requirements for those with roles in incident reporting. Core training on the action plans and procedures to recover or re-establish BES Cyber Systems for personnel having a role in the recovery; FERC Order No. 706, Paragraph 413. Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems; FERC Order No. 706, Paragraph 434.

Reference to prior version: (Part 2.2) CIP004-4, R2.1

Change Rationale: (Part 2.2)

Addition of exceptional circumstances parameters as directed in FERC Order No. 706, Paragraph 431 is detailed in CIP-003-5.

Reference to prior version: (Part 2.3) CIP004-4, R2.3

Change Rationale: (Part 2.3)

Updated to replace "annually" with "once every 15 calendar months."

Rationale for R3:

To ensure that individuals who need authorized electronic or authorized unescorted physical access to BES Cyber Systems have been assessed for risk. Whether initial access or maintaining access, those with access must have had a personnel risk assessment completed within the last 7 years.

Summary of Changes: Specify that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more, including current residence regardless of duration.

Reference to prior version: (Part 3.1) CIP004-4, R3.1

Change Rationale: (Part 3.1)

Addressed interpretation request in guidance. Specified that process for identity confirmation is required. The implementation plan clarifies that a documented identity verification conducted under an earlier version of the CIP standards is sufficient.

Reference to prior version: (Part 3.2) CIP004-4, R3.1

Change Rationale: (Part 3.2)

Specify that the seven year criminal history check covers all locations where the individual has resided for six months or more, including current residence regardless of duration. Added

additional wording based on interpretation request. Provision is made for when a full seven-year check cannot be performed.

Reference to prior version: (Part 3.3) New

Change Rationale: (Part 3.3)

There should be documented criteria or a process used to evaluate criminal history records checks for authorizing access.

Reference to prior version: (Part 3.4) CIP-004-4, R3.3

Change Rationale: (Part 3.4)

Separated into its own table item.

Reference to prior version: (Part 3.5) CIP-004-3, R3, R3.3

Change Rationale: (Part 3.5)

Whether for initial access or maintaining access, establishes that those with access must have had PRA completed within 7 years. This covers both initial and renewal. The implementation plan specifies that initial performance of this requirement is 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment. CIP-004-3, R3, R3.3

Rationale for R4:

To ensure that individuals with access to BES Cyber Systems and the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity have been properly authorized for such access. "Authorization" should be considered to be a grant of permission by a person or persons empowered by the Responsible Entity to perform such grants and included in the delegations referenced in CIP-003-5. "Provisioning" should be considered the actions to provide access to an individual.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (i.e., physical access control system, remote access system, directory services).

CIP Exceptional Circumstances are defined in a Responsible Entity's policy from CIP-003-5 and allow an exception to the requirement for authorization to BES Cyber Systems and BES Cyber System Information.

Quarterly reviews in Part 4.5 are to perform a validation that only authorized users have been granted access to BES Cyber Systems. This is achieved by comparing individuals actually provisioned to a BES Cyber System against records of individuals authorized to access the BES Cyber System. The focus of this requirement is on the integrity of provisioning access rather than individual accounts on all BES Cyber Assets. The list of provisioned individuals can be an automatically generated account listing. However, in a BES Cyber System with several account

databases, the list of provisioned individuals may come from other records such as provisioning workflow or a user account database where provisioning typically initiates.

If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the SDT intends that the error should not be considered a violation of this requirement.

For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R4 are not applicable. However, the Responsible Entity should document such configurations.

Summary of Changes: The primary change was in pulling the access management requirements from CIP-003-4, CIP-004-4, and CIP-007-4 into a single requirement. The requirements from Version 4 remain largely unchanged except to clarify some terminology. The purpose for combining these requirements is to remove the perceived redundancy in authorization and review. The requirement in CIP-004-4 R4 to maintain a list of authorized personnel has been removed because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access.

Reference to prior version: (Part 4.1) CIP 003-4, R5.1 and R5.2; CIP-006-4, R1.5 and R4; CIP-007-4, R5.1 and R5.1.1

Change Rationale: (Part 4.1)

Combined requirements from CIP-003-4, CIP-007-4, and CIP-006-4 to make the authorization process clear and consistent. *CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 all reference authorization of access in some form, and CIP-003-4 and CIP-007-4 require authorization on a "need to know" basis or with respect to work functions performed. These were consolidated to ensure consistency in the requirement language.*

Reference to prior version: (Part 4.2) CIP 004-4, R4.1

Change Rationale: (Part 4.2)

Feedback among team members, observers, and regional CIP auditors indicates there has been confusion in implementation around what the term "review" entailed in CIP-004-4, Requirement R4.1. This requirement clarifies the review should occur between the provisioned access and authorized access.

Reference to prior version: (Part 4.3) CIP 007-4, R5.1.3

Change Rationale: (Part 4.3)

Moved requirements to ensure consistency and eliminate the cross-referencing of requirements. Clarified what was necessary in performing verification by stating the objective was to confirm that access privileges are correct and the minimum necessary.

Reference to prior version: (Part 4.4) CIP-003-4, R5.1.2

Change Rationale: (Part 4.4)

Moved requirement to ensure consistency among access reviews. Clarified precise meaning of annual. Clarified what was necessary in performing a verification by stating the objective was to

confirm access privileges are correct and the minimum necessary for performing assigned work functions.

Rationale for R5:

The timely revocation of electronic access to BES Cyber Systems is an essential element of an access management regime. When an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked. This is of particular importance in situations where a change of assignment or employment is involuntary, as there is a risk the individual(s) involved will react in a hostile or destructive manner.

In considering how to address directives in FERC Order No. 706 directing "immediate" revocation of access for involuntary separation, the SDT chose not to specify hourly time parameters in the requirement (e.g., revoking access within 1 hour). The point in time at which an organization terminates a person cannot generally be determined down to the hour. However, most organizations have formal termination processes, and the timeliest revocation of access occurs in concurrence with the initial processes of termination.

Access is physical, logical, and remote permissions granted to Cyber Assets composing the BES Cyber System or allowing access to the BES Cyber System. When granting, reviewing, or revoking access, the Responsible Entity must address the Cyber Asset specifically as well as the systems used to enable such access (e.g., physical access control system, remote access system, directory services).

Summary of Changes: FERC Order No. 706, Paragraphs 460 and 461, state the following: "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a Critical Cyber Asset for any reason (including disciplinary action, transfer, retirement, or termination).

As a general matter, the Commission believes that revoking access when an employee no longer needs it, either because of a change in job or the end of employment, must be immediate."

Reference to prior version: (Part 5.1) CIP 004-4, R4.2

Change Rationale: (Part 5.1)

The FERC Order No. 706, Paragraphs 460 and 461, directs modifications to the Standards ***to require immediate revocation*** *for any person no longer needing access. To address this directive, this requirement specifies revocation concurrent with the termination instead of within 24 hours.*

Reference to prior version: (Part 5.2) CIP-004-4, R4.2

Change Rationale: (Part 5.2)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access, including transferred employees. In reviewing how to modify this requirement, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement from NIST 800-53 Version 3 to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers.

Reference to prior version: (Part 5.3) New

Change Rationale: (Part 5.3)

FERC Order No. 706, Paragraph 386, directs modifications to the standards to require prompt revocation of access to protected information. To address this directive, Responsible Entities are required to revoke access to areas designated for BES Cyber System Information. This could include records closets, substation control houses, records management systems, file shares or other physical and logical areas under the Responsible Entity's control.

Reference to prior version: (Part 5.4) New

Change Rationale: (Part 5.4)

FERC Order No. 706, Paragraph 460 and 461, direct modifications to the Standards to require immediate revocation for any person no longer needing access. In order to meet the immediate timeframe, Responsible Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.

Reference to prior version: (Part 5.5) CIP-007-4, R5.2.3

Change Rationale: (Part 5.5)

To provide clarification of expected actions in managing the passwords.

Version History

Version	Date	Action	Change Tracking
1	~~01~~1/16/06	~~D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…"~~R3.2 — Change "Control Center" to "control center."	~~03~~3/24/06
~~1~~2	~~06/01/06~~9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~D.2.1.4 — Change "access control rights" to "access rights."~~ Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	~~06/05/06~~
~~2~~3	12/16/09	**Updated version number from -2 to -3 Approved by the NERC Board of Trustees.** ~~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.~~ ~~Reference to emergency situations.~~ ~~Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.~~ ~~Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.~~ ~~Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to~~	

		~~"Critical Cyber Assets".~~ ~~Removal of 90-day window to complete training and 30-day window to complete personnel risk assessments.~~ ~~**Changed compliance monitor to Compliance Enforcement Authority.**~~	
3	3/31/10	Approved by FERC.~~Update~~ ~~**version number from -2 to -3**~~	
~~3~~4	12/~~16/09~~30/10	~~**Approved by NERC Board of Trustees**~~Modified to add specific criteria for Critical Asset identification.	Update
4	~~Board approved~~ ~~01~~1/24/~~2011~~11	~~**Update version number from "3" to "4"**~~Approved by the NERC Board of Trustees.	Update~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~
~~4~~5	~~**4/19**~~11/26/12	~~FERC Order issued approving CIP-004-4 (approval becomes effective June 25, 2012)~~ ~~**Added approved VRF/VSL table to section D.2.**~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

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

2. Number: CIP-005-5

3. Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-005-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the

Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

E*xplicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.*

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

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

2. Number: CIP-005-~~4a~~5

3. Purpose: ~~Standard CIP-005-4a requires the identification and protection of the~~ To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter~~(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.~~ in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard ~~CIP-005-4a should be read as part of a~~ .

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

~~3.~~4.1.2.4 Each Cranking Path and group of ~~standards numbered Standards CIP-002-4 through CIP-009-4.~~ Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

~~**4. Applicability**~~

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

4.1.3 ~~Reliability~~**Generator Operator**

4.1.4 Generator Owner

~~**4.1.1 Interchange** **Coordinator.**~~

~~**4.1.2 Balancing Authority.**~~

~~**4.1.3**~~**4.1.5 or Interchange Authority**~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6 Reliability Coordinator

~~**4.1.5**~~**4.1.7 Transmission** ~~Owner.~~**Operator**

~~**4.1.6 Transmission** Operator.~~

~~**4.1.7**~~**4.1.8** ~~Generator~~ **Owner**~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.~~4.2.3 Exemptions: The following are exempt from Standard CIP-005-~~4a:~~5:

~~4.2.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~4.2.3.2 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~~4.2.3.3 ~~In nuclear plants, the~~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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ ~~The~~ Dates:

1. **24 Months Minimum** – CIP-005-5 shall become effective on the later of July 1, 2015, or the first ~~day of the eighth~~ calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective~~ approval.

~~5.~~ 2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter ~~after BOT adoption in those jurisdictions where regulatory approval is not required).~~ following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~**B. Requirements**~~

~~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).~~

~~a. 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).~~

~~b. 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.~~

~~c. 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).~~

~~d. 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.~~

~~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.~~

~~e. 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.~~

~~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).~~

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

~~g. 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.~~

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

~~i. 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.~~

~~j. The required documentation shall, at least, identify and describe:~~

i. The processes for access request and authorization.

ii. The authentication methods.

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

iv. The controls used to secure dial-up accessible connections.

k. 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.

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.

l. 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.

m. 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.

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:

n. A document identifying the vulnerability assessment process;

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

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

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

r. 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.

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.

~~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.~~

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

~~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.~~

6. Background:

Standard CIP-005-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident

response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-5 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R1 – Electronic Security Perimeter

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-5 Table R2 – Interactive Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-5 Table R2 – Interactive Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

~~D.~~C. 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~~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,~~ ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. ~~For the ERO, a third-party monitor without vested interest~~**Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in ~~the outcome~~this standard for ~~the ERO~~three calendar years.

~~**1.2.4**~~• If a Responsible Entity is found non-compliant, it shall ~~serve as~~keep information related to the non-compliance until mitigation is complete and approved or for the ~~Compliance Enforcement Authority~~time specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Enforcement~~Assessment Processes:

- Compliance ~~Audits~~Audit
- Self-~~Certifications~~Certification
- Spot Checking

- Compliance Violation InvestigationsInvestigation
- 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.

- Complaint

1.5.1.4. 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	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	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;	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	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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; and Standard CIP-009-4.	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; 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.	Requirement R3; Standard CIP-007-4 Requirements R1 and R3 through R9; Standard CIP-008-4; 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.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
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 Perimeter.	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.
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

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
R2.6.	LOWER	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.
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	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.

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
		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.			
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 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
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

Requirement	VRF	Lower VSL	Moderate VSL	High VSL	Severe VSL
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.
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.

- None

~~E.~~D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the

Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)

Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)

Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)

Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)

Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)

Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:

Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed

to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Version History

Version	Date	Action	Change Tracking
1	~~01~~1/16/06	~~D~~R3.2.~~3.1~~ — Change "~~Critical Assets,"~~Control Center" to "~~Critical Cyber Assets" as intended.~~control center."	~~03~~3/24/06
2	~~Approved by NERC Board of Trustees 5/6/09~~9/30/09	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).~~	~~Revised.~~

		Changed compliance monitor to Compliance Enforcement Authority.	
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."**~~Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	~~**Conforming revisions for FERC Order on CIP V2 Standards (9/30/2009)**~~
~~2a~~3	~~02/16~~3/31/10	~~**Added Appendix 1 – Interpretation of R1.3 approved by BOT on February 16, 2010**~~Approved by FERC.	~~**Addition**~~
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
~~4a~~5	~~01/24/~~11/26/12	Adopted by the NERC Board of Trustees.	**Modified to coordinate with other CIP standards and to revise format to use RBS Template.**~~**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 — Physical Security of BES Cyber Systems

2. Number: CIP-006-5

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-006-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1– Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- 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 into the Physical Security Perimeter.

Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for notification within 15 minutes to individuals responsible for response.
- Human Observation of Access Points: Monitoring of physical access points by security personnel who are also controlling physical access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and alerting method.
- Video Recording: Electronic capture of video images of 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.

The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of contact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Each Responsible Entity shall ensure that physical access to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.*

Summary of Changes: The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

Added details to address FERC Order No. 706, Paragraph 572, directives for physical security defense in depth.

Additional guidance on physical security defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity*

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

Added to address FERC Order No. 706, Paragraph 572, related directives for physical security defense in depth.
FERC Order No. 706, Paragraph 575, directives addressed by providing the examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).

Reference to prior version: (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

CIP-006-4c, Requirement R6 was specific to the logging of access at identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated Version Number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: ~~———~~Cyber Security — Physical Security of ~~Critical~~BES Cyber ~~Assets~~Systems

2. Number: CIP-006-~~4c~~5

~~**3. Purpose:** Standard CIP-006-4c is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.~~

3. Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

~~**4.1.** Within the text of Standard CIP-006-4c, "Responsible Entity" shall mean:~~

~~**4.1.1** Reliability Coordinator~~

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

~~**4.1.2 Transmission Service Provider**~~

4.1.6 Reliability Coordinator

4.1.7 Transmission ~~Owner~~Operator

~~**4.1.3 Transmission Operator**~~

4.1.8 ~~Generator~~ Owner

~~**4.1.4 Generator Operator**~~

~~**4.1.5 Load Serving Entity**~~

~~**4.1.6 NERC**~~

~~**4.1.7 Regional Entity**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-006-~~4c:~~5:

~~4.2.1~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~**4.2.3.3** ~~In nuclear plants, the~~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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~4.2.4~~**4.2.3.5** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical Cyber Assets~~BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ ~~The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes~~**Dates:**

1. **24 Months Minimum** – CIP-006-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after ~~BOT adoption in~~ the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is ~~not~~ required~~).~~, CIP-006-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~B. Requirements~~

~~**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:~~

~~**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.~~

~~**R1.2.** Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.~~

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

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.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-4 Requirement R4.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

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.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

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.

R1.8. Annual review of the physical security plan.

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:

R2.1. Be protected from unauthorized physical access.

Be afforded the protective measures specified in Standard CIP-003-4; **6. Background:**

R2.2. Standard CIP-004-4 Requirement R3; Standard006-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-4a Requirements R2 and R3; Standard CIP-006-4c Requirements R4 and R5; Standard5, CIP-006-5, CIP-007-4; Standard5, CIP-008-4; and Standard5, CIP-009-4.

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.

Physical Access Controls — The Responsible Entity shall document and implement the5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, 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. Themitigate risk to

BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each* *Responsible Entity shall implement one or more* ~~of the~~*documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems without External Routable Connectivity** – Only applies to medium impact BES Cyber Systems without External Routable Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may

include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Locally mounted hardware or devices at the Physical Security Perimeter –** Applies to the locally mounted hardware or devices (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) at a Physical Security Perimeter associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity, and that does not contain or store access control information or independently perform access authentication. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].*

M1. Evidence must include each of the documented physical security plans that collectively include all of the applicable requirement parts in *CIP-006-5 Table R1 – Physical Security Plan* and additional evidence to demonstrate implementation of the plan or plans as described in the Measures column of the table.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	Medium Impact BES Cyber Systems without External Routable Connectivity Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Define operational or procedural controls to restrict physical access.	An example of evidence may include, but is not limited to, documentation that operational or procedural controls exist.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how unescorted physical access is controlled by one or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the Physical Security Perimeters and how unescorted physical access is controlled by two or more different methods and proof that unescorted physical access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by access logs.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized access through a physical access point into a Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized access through a physical access control into a Physical Security Perimeter and additional evidence that the alarm or alert was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as manual or electronic alarm or alert logs, cell phone or pager logs, or other evidence that documents that the alarm or alert was generated and communicated.
1.6	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	An example of evidence may include, but is not limited to, documentation of controls that monitor for unauthorized physical access to a PACS.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.7	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	An example of evidence may include, but is not limited to, language in the physical security plan that describes the issuance of an alarm or alert in response to unauthorized physical access to Physical Access Control Systems and additional evidence that the alarm or alerts was issued and communicated as identified in the BES Cyber Security Incident Response Plan, such as alarm or alert logs, cell phone or pager logs, or other evidence that the alarm or alert was generated and communicated.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.8	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	An example of evidence may include, but is not limited to, language in the physical security plan that describes logging and recording of physical entry into each Physical Security Perimeter and additional evidence to demonstrate that this logging has been implemented, such as logs of physical access into Physical Security Perimeters that show the individual and the date and time of entry into Physical Security Perimeter.

CIP-006-5 Table R1 – Physical Security Plan			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.9	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	An example of evidence may include, but is not limited to, dated documentation such as logs of physical access into Physical Security Perimeters that show the date and time of entry into Physical Security Perimeter.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented visitor control programs that include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M2. Evidence must include one or more documented visitor control programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R2 – Visitor Control Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as visitor logs.

CIP-006-5 Table R2 – Visitor Control Program			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	An example of evidence may include, but is not limited to, language in a visitor control program that requires continuous escorted access of visitors within Physical Security Perimeters and additional evidence to demonstrate that the process was implemented, such as dated visitor logs that include the required information.
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; and 2. PCA	Retain visitor logs for at least ninety calendar days.	An example of evidence may include, but is not limited to, documentation showing logs have been retained for at least ninety calendar days.

R3. Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M3. Evidence must include each of the documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable requirement parts in *CIP-006-5 Table R3 – Maintenance and Testing Program* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-006-5 Table R3 – Physical Access Control System Maintenance and Testing Program			
Part	**Applicable Systems**	**Requirement**	**Measures**
3.1	Physical Access Control Systems (PACS) associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity Locally mounted hardware or devices at the Physical Security Perimeter associated with: • High Impact BES Cyber Systems, or • Medium Impact BES Cyber Systems with External Routable Connectivity	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	An example of evidence may include, but is not limited to, a maintenance and testing program that provides for testing each Physical Access Control System and locally mounted hardware or devices associated with each applicable Physical Security Perimeter at least once every 24 calendar months and additional evidence to demonstrate that this testing was done, such as dated maintenance records, or other documentation showing testing and maintenance has been performed on each applicable device or system at least once every 24 calendar months.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

~~**R4.**~~ The following ~~physical access methods:~~evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

General:

While the focus is shifted from the definition and management of a completely enclosed "six-wall" boundary, it is expected in many instances this will remain a primary mechanism for controlling, alerting, and logging access to BES Cyber Systems. Taken together, these controls will effectively constitute the physical security plan to manage physical access to BES Cyber Systems.

Requirement R1:

Methods of physical access control include:

- 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~~into the ~~Critical Cyber Assets.~~Physical Security Perimeter.

~~**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~~ Methods to monitor physical access include:

- Alarm Systems: Systems that alarm to indicate interior motion or when a door, gate, or window has been opened without authorization. These alarms must provide for ~~immediate~~ notification within 15 minutes to ~~personnel~~individuals responsible for response.
- Human Observation of Access Points: ~~-~~Monitoring of physical access points by ~~authorized~~security personnel ~~as specified in Requirement R4.~~

~~**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~~who are also controlling physical ~~entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:~~access.

Methods to log physical access include:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and ~~monitoring~~alerting method.
- Video Recording: Electronic capture of video images of 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~~.

~~**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-008-4.~~

~~**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:~~

~~**R8.1.** Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.~~

~~**R8.2.** Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.~~

~~**R8.3.** Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.~~

~~C. Measures~~

M1. The Responsible Entity shall make available the physical security plan as specified in Requirement R1 and documentation of the implementation, review and updating of the plan.

M2. The Responsible Entity shall make available documentation that the physical access control systems are protected as specified in Requirement R2.

M3. The Responsible Entity shall make available documentation that the electronic access control systems are located within an identified Physical Security Perimeter as specified in Requirement R3.

The Responsible Entity shall make available documentation identifying the methods for The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are), or a physical key in combination with a guard-monitored remote camera and door release, where the "guard" has adequate information to authenticate the person they are observing or talking to prior to permitting access (something you have and something you are). The two-factor authentication could be implemented using a single Physical Access Control System but more than one authentication method must be utilized. For physically layered protection, a locked gate in combination with a locked control-building could be acceptable, provided no single authenticator (e.g., key or card key) would provide access through both.

Entities may choose for certain PACS to reside in a PSP controlling physical access to access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

Requirement R2:

The logging of visitors should capture each access visit of the individual and does not need to capture each entry or exit during that visit. This is meant to allow a visitor to temporarily exit the Physical Security Perimeter to obtain something they left in their vehicle or outside the area without requiring a new log entry for each and every entry during the visit.

The SDT also determined that a point of acontact should be documented who can provide additional details about the visit if questions arise in the future. The point of contact could be the escort, but there is no need to document everyone that acted as an escort for the visitor.

Requirement R3:

M4. This includes the testing of locally mounted hardware or devices used in controlling, alerting or logging access to the Physical Security Perimeter as specified in Requirement R4. This includes motion sensors, electronic lock control mechanisms, and badge readers which are not deemed to be part of the Physical Access Control System but are required for the protection of the BES Cyber Systems.

~~The~~Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

~~**M5.**~~ Each Responsible Entity shall ~~make available documentation identifying the methods for monitoring~~ensure that physical access ~~as specified~~to all BES Cyber Systems is restricted and appropriately managed. *Entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement ~~R5~~Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP*.

~~**M6.** The Responsible Entity shall make available documentation identifying the methods for logging physical access as specified in Requirement R6.~~

~~**M7.** The Responsible Entity shall make available documentation to show retention of access logs as specified in Requirement R7.~~

~~The Responsible Entity shall make available documentation to show its implementation of a~~ **Summary of Changes:** The entire content of CIP-006-5 is intended to constitute a physical security program. This represents a change from previous versions, since there was no specific requirement to have a physical security program in previous versions of the standards, only requirements for physical security plans.

~~**M8.**~~ Added details to address FERC Order No. 706, Paragraph 572, directives for physical security ~~system maintenance and testing program as specified~~defense in ~~Requirement R8.~~

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 documents other than those specified in Requirements R7 and R8.2 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 recordsdepth.

1.5. Additional Compliance Information

~~The Responsible Entity may not make exceptions in its cyber~~ guidance on physical security ~~policy to the creation, documentation, or maintenance of a~~ defense in depth provided to address the directive in FERC Order No. 706, Paragraph 575.

Reference to prior version: (Part 1.1) *CIP-006-4c, R2.1 for Physical Access Control Systems*
New Requirement for Medium Impact BES Cyber Systems not having External Routable Connectivity

Change Rationale: (Part 1.1)

To allow for programmatic protection controls as a baseline (which also includes how the entity plans to protect Medium Impact BES Cyber Systems that do not have External Routable Connectivity not otherwise covered under Part 1.2, and it does not require a detailed list of individuals with access). Physical Access Control Systems do not themselves need to be protected at the same level as required in Parts 1.2 through 1.5.

Reference to prior version: (Part 1.2) CIP006-4c, R3 & R4
Change Rationale: (Part 1.2)

This requirement has been made more general to allow for alternate measures of restricting physical access. Specific examples of methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.3) CIP006-4c, R3 & R4

Change Rationale: (Part 1.3)

The specific examples that specify methods a Responsible Entity can take to restricting access to BES Cyber Systems has been moved to the Guidelines and Technical Basis section. This requirement has been made more general to allow for alternate measures of controlling physical access.

~~**1.5.1**~~ *Added to address FERC Order No. 706, Paragraph 572, related directives for physical security* ~~plan~~*defense in depth*.
~~For dial-up accessible Critical Cyber Assets that use non-routable protocols,~~*FERC Order No. 706, Paragraph 575, directives addressed by providing the* ~~Responsible Entity shall not be required~~*examples in the guidance document of physical security defense in depth via multi-factor authentication or layered Physical Security Perimeter(s).*

Reference **to** ~~comply with Standard~~**prior version:** (Part 1.4) CIP006-4c, R5

Change Rationale: (Part 1.4)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.5) CIP006-4c, R5

Change Rationale: (Part 1.5)

Examples of monitoring methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.6) CIP006-4c, R5

Change Rationale: (Part 1.6)

Addresses the prior CIP-006-4c, Requirement R5 requirement for ~~that single~~Physical Access Control Systems.

Reference to prior version: (Part 1.7) CIP006-4c, R5

Change Rationale: (Part 1.7)

Addresses the prior CIP-006-4c, Requirement R5 requirement for Physical Access Control Systems.

Reference to prior version: (Part 1.8) CIP-006-4c, R6

Change Rationale: (Part 1.8)

~~**1.5.2**~~ *CIP-006-4c, Requirement R6 was specific to the logging of access ~~point~~ at ~~the dial-up device.~~identified access points. This requirement more generally requires logging of authorized physical access into the Physical Security Perimeter.*

~~2. Violation Severity Levels~~

~~Requirement~~	~~VRF~~	~~Lower VSL~~	~~Moderate VSL~~	~~High VSL~~	~~Severe VSL~~
~~R1.~~	~~MEDIUM~~	~~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.~~

~~R1.1.~~	~~MEDIUM~~	~~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.~~
~~R1.2.~~	~~MEDIUM~~	~~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 Security Perimeter.~~	~~The Responsible Entity's physical security identifies all access points through each Physical Security Perimeter but does not identify measures to control entry at those access points.~~	~~The Responsible Entity's physical security plan does not identify all access points through each Physical Security Perimeter nor measures to control entry at those access points.~~
~~R1.3~~	~~MEDIUM~~	~~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).~~
~~R1.4~~	~~MEDIUM~~	~~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.~~
~~R1.5~~	~~MEDIUM~~	~~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.~~
~~R1.6~~	~~MEDIUM~~	~~The responsible Entity included a 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.~~	~~The responsible Entity included a visitor control program in its physical security plan, but either did not log the visitor or did not log the escort.~~	~~The responsible Entity included a visitor control program in its physical security plan, but it does not meet the requirements of continuous escort.~~	~~The Responsible Entity did not include or implement a visitor control program in its physical security plan.~~
~~R1.6.1~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~R1.6.2~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.7~~	~~LOWER~~	~~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 reconfiguration.~~	~~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.~~
~~R1.8~~	~~LOWER~~	~~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.~~
~~R2~~	~~MEDIUM~~	~~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 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 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 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 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 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.~~
~~R2.1.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R2.2.~~	~~MEDIUM~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

R3	MEDIUM	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 an identified Physical Security Perimeter.
R4	MEDIUM	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 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.	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: 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.	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: 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..
R5	MEDIUM	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	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 notification to personnel	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 notification to personnel responsible

			~~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 points by authorized personnel as specified in Requirement R4.~~	~~responsible for response.~~ ~~• Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.~~	~~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.~~
~~R6~~	~~LOWER~~	~~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 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~~	~~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 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..~~	~~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 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.~~	~~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 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.~~

		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.			
R7	LOWER	The Responsible Entity retained physical access logs for 75 or more calendar days, but for less than 90 calendar days.	The Responsible Entity retained physical access logs for 60 or more calendar days, but for less than 75 calendar days.	The Responsible Entity retained physical access logs for 45 or more calendar days, but for less than 60 calendar days.	The Responsible Entity retained physical access logs for less than 45 calendar days.
R8	MEDIUM	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.
R8.1	MEDIUM	N/A	N/A	N/A	N/A
R8.2	LOWER	N/A	N/A	N/A	N/A
R8.3	LOWER	N/A	N/A	N/A	N/A

E. Regional Variances

None identified.

Examples of logging methods have been moved to the Guidelines and Technical Basis section.

Reference to prior version: (Part 1.9) CIP-006-4c, R7

Change Rationale: (Part 1.9)

No change.

Rationale for R2:

To control when personnel without authorized unescorted physical access can be in any Physical Security Perimeters protecting BES Cyber Systems or Electronic Access Control or Monitoring Systems, as applicable in Table R2.

Summary of Changes: Reformatted into table structure. Originally added in Version 3 per FERC Order issued September 30, 2009.

Reference to prior version: (Part 2.1) CIP-006-4c, R1.6.2

Change Rationale: (Part 2.1)

Added the ability to not do this during CIP Exceptional Circumstances.

Reference to prior version: (Part 2.2) CIP-006-4c R1.6.1

Change Rationale: (Part 2.2)

Added the ability to not do this during CIP Exceptional Circumstances, addressed multi-entry scenarios of the same person in a day (log first entry and last exit), and name of the person who is responsible or sponsor for the visitor. There is no requirement to document the escort or handoffs between escorts.

Reference to prior version: (Part 2.3) CIP-006-4c, R7

Change Rationale: (Part 2.3)

No change

Rationale for R3:

To ensure all Physical Access Control Systems and devices continue to function properly.

Summary of Changes: Reformatted into table structure.

Added details to address FERC Order No. 706, Paragraph 581, directives to test more frequently than every three years.

Reference to prior version: (Part 3.1) CIP-006-4c, R8.1 and R8.2

Change Rationale: (Part 3.1)

Added details to address FERC Order No. 706, Paragraph 581 directives to test more frequently than every three years. The SDT determined that annual testing was too often and agreed on two years.

Version History

Version	Date	Action	Change Tracking
~~1~~	~~May 2, 2006~~	~~Adopted by NERC Board of Trustees~~	
1	~~**January 18, 2008**~~1/16/06	~~**FERC Order issued approving CIP-006-1**~~R3.2 — Change "Control Center" to "control center."	3/24/06
	~~February 12, 2008~~	~~Interpretation of R1 and Additional Compliance Information Section 1.4.4 adopted by NERC Board of Trustees~~	~~Project 2007-27~~
2	9/30/09	~~Updated version number from -1 to -2~~ Modifications to ~~**remove extraneous information from**~~clarify the requirements~~**, improve readability,**~~ 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. Changed compliance monitor to Compliance Enforcement Authority.	~~**Project 2008-06**~~
~~2~~	~~May 6, 2009~~	~~Adopted by NERC Board of Trustees~~	
	~~August 5, 2009~~	~~Interpretation of R4 adopted by NERC Board of Trustees~~	~~Project 2008-15~~
~~2~~	~~September 30, 2009~~	~~FERC Order issued approving CIP-006-2~~	
3	~~**November 18, 2009**~~12/16/09	Updated ~~**version number**~~Version Number from -2 to -3	~~**Project 2009-21**~~

Version	Date	Action	Change Tracking
		~~Revised~~In Requirement 1.6, deleted the sentence pertaining to ~~add a Visitor Control program~~removing component or system from service in order to ~~the Physical Security Plan~~perform testing, in response to FERC order issued September 30, 2009. ~~In Requirement R7, the term "Responsible Entity" was capitalized. Updated Requirements R1.6.1 and R1.6.2 to be responsive to FERC Order RD09-7~~	
~~3~~	~~December 16, 2009~~	~~Adopted by NERC Board of Trustees~~	
3	~~February~~ 12/16~~,~~ ~~2010~~/09	~~Interpretation of R1 and R1.1 adopted~~Approved by the NERC Board of Trustees~~.~~.	~~Project 2009-13~~
3	~~March~~ 3/31~~,~~ ~~2010~~/10	~~FERC Order issued approving CIP-006-3~~Approved by FERC.	
~~2a/3a~~	~~July 15, 2010~~	~~FERC Order issued approving the Interpretation of R1 and R1.1.~~ ~~Updated version numbers from 2/3 to 2a/3a.~~	
4	~~January~~ 1/24~~,~~ ~~2011~~/11	~~Adopted~~Approved by the NERC Board of Trustees.	
~~3c/4c~~5	~~May 19, 2011~~11/26/12	~~FERC Order issued approving two interpretations: 1) Interpretation of R1 and Additional Compliance Information Section 1.4.4; and 2) Interpretation of R4.~~ ~~Updated version number from 3/4 to 3c/4c.~~Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
~~4c~~	~~4/19/12~~	~~FERC Order issued approving CIP-006-4c (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

~~Appendix 1~~

~~Requirement Number and Text of Requirement~~
~~R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:~~ ~~R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.~~
~~**Question**~~
~~If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?~~ ~~Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?~~
~~**Response**~~
~~For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.~~

Appendix 2

Interpretation of Requirement R1.1.

Request: *Are dial-up RTUs that use non-routable protocols and have dial-up access required to have a six-wall perimeters or are they exempted from CIP-006-1 and required to have only electronic security perimeters? This has a direct impact on how any identified RTUs will be physically secured.*

Interpretation:

Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-1, and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border.

CIP-006-1 — Requirement 1.1 requires a Responsible Entity to have a physical security plan that stipulate cyber assets that are within the Electronic Security Perimeter also be within a Physical Security Perimeter.

> **R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:**
>
> **R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.**

CIP-006-1 — Additional Compliance Information 1.4.4 identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.

> **1.4. Additional Compliance Information**
>
> **1.4.4 For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.**

Appendix 3

The following interpretation of CIP-006-1a — Cyber Security — Physical Security of Critical Cyber Assets, Requirement R4 was developed by the standard drafting team assigned to Project 2008-14 (Cyber Security Violation Severity Levels) on October 23, 2008.

Request:

1. *For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?*
2. *Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?*

Interpretation:

No, monitoring and logging of access are only required for ingress at this time. The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Requirement Number and Text of Requirement

R4. 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:

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. 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 R2.3.

A. Introduction

1. Title: Cyber Security — System Security Management

2. Number: CIP-007-5

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-007-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact

and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP_Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter in which

case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security patches. The requirement applies to patches only,

which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. 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. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 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.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as

it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include:

(i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit purposes, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

4.4. Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports.

The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.

Reference to prior version: (Part 1.1) CIP-007-4, R2.1 and R2.2

Change Rationale: (Part 1.1)

The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.

Reference to prior version: (Part 1.2) New

Change Rationale: (Part 1.2)

On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Rationale for R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

Summary of Changes: The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security

upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

Reference to prior version: (Part 2.1) CIP-007, R3

Change Rationale: (Part 2.1)

The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.

Reference to prior version: (Part 2.2) CIP-007, R3.1

Change Rationale: (Part 2.2)

Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.

Reference to prior version: (Part 2.3) CIP-007, R3.2

Change Rationale: (Part 2.3)

The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.

Reference to prior version: (Part 2.4) CIP-007, R3.2

Change Rationale: (Part 2.4)

Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.

Rationale for R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of

that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Reference to prior version: (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1

Change Rationale: (Part 3.1)

See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.

Reference to prior version: (Part 3.2) *CIP-007-4, R4; CIP-007-4, R4.1*
Change Rationale: (Part 3.2)

See the Summary of Changes.

Reference to prior version: (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2

Change Rationale: (Part 3.3)

Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.

Rationale for R4:

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor."

The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

Reference to prior version: (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3

Change Rationale: (Part 4.1)

This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.

Reference to prior version: (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2

Change Rationale: (Part 4.2)

This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.

Reference to prior version: (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4

Change Rationale: (Part 4.3)

No substantive change.

Reference to prior version: (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5

Change Rationale: (Part 4.4)

Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information.

Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.

Rationale for R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term “authorized” is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for

true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication

mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

Reference to prior version: (Part 5.1) CIP-007-4, R5

Change Rationale: (Part 5.1)

The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document controls is included in this introductory requirement. The requirement to have technical and procedural controls was removed because technical controls suffice when procedural documentation is already required. The phrase "that minimize the risk of unauthorized access" was removed and more appropriately captured in the rationale statement.

Reference to prior version: (Part 5.2) CIP-007-4, R5.2 and R5.2.1

Change Rationale: (Part 5.2)

CIP-007-4 requires entities to minimize and manage the scope and acceptable use of account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.

Reference to prior version: (Part 5.3) CIP-007-4, R5.2.2

Change Rationale: (Part 5.3)

No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

Reference to prior version: (Part 5.4) CIP-007-4, R5.2.1

Change Rationale: (Part 5.4)

The requirement for the "removal, disabling or renaming of such accounts where possible" has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords to permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.

Reference to prior version: (Part 5.5) CIP-007-4, R5.3

Change Rationale: (Part 5.5)

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password

credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.

Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3

Change Rationale: (Part 5.6)

**This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

Reference to prior version: (Part 5.7) *New Requirement*

Change Rationale: (Part 5.7)

Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	

3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — SystemsSystem Security Management

2. Number: CIP-007-45

~~**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.~~

3. Purpose: To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

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

4.1. ~~Reliability~~ **Functional Entities:** For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.1 Interchange Coordinator.

4.1.2 Balancing Authority.

4.1.34.1.5 or Interchange Authority.

4.1.4 Transmission Service Provider.

4.1.6 Reliability Coordinator

4.1.54.1.7 Transmission Owner.Operator

4.1.6 Transmission Operator.

4.1.74.1.8 Generator Owner.

4.1.8 Generator Operator.

4.1.9 Load Serving Entity.

4.1.10 NERC.

4.1.11 Regional Entity.

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~**4.2.**~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-007-~~4:~~5:

~~**4.2.1**~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.2.2**~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.2.3**~~**4.2.3.3** ~~In nuclear plants, the~~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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.4**~~**4.2.3.5** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical Cyber Assets~~BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ ~~The~~ Dates:

1. **24 Months Minimum** – CIP-007-5 shall become effective on the later of July 1, 2015, or the first ~~day of the eighth~~ calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective~~ approval.

~~**5.**~~ 2. In those jurisdictions where no regulatory approval is required, CIP-007-5 shall become effective on the first day of the ninth calendar quarter ~~after BOT adoption in those jurisdictions where regulatory approval is not required).~~following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

~~B. Requirements~~

~~Test Procedures — The~~ **6. Background:**

Standard CIP-007-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural

controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall* ensure that new*implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets ~~and significant changes to existing~~in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System in the applicability column. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Protected Cyber Assets** ~~within the Electronic~~ **(PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]*

M1. Evidence must include the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R1 – Ports and Services* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	Examples of evidence may include, but are not limited to: • Documentation of the need for all enabled ports on all applicable Cyber Assets and Electronic Access Points, individually or by group. • Listings of the listening ports on the Cyber Assets, individually or by group, from either the device configuration files, command output (such as netstat), or network scans of open ports; or • Configuration files of host-based firewalls or other device level mechanisms that only allow needed ports and deny all others.

CIP-007-5 Table R1– Ports and Services			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems at Control Centers	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	An example of evidence may include, but is not limited to, documentation showing types of protection of physical input/output ports, either logically through system configuration or physically using a port lock or signage.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	An example of evidence may include, but is not limited to, an evaluation conducted by, referenced by, or on behalf of a Responsible Entity of security-related patches released by the documented sources at least once every 35 calendar days.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Examples of evidence may include, but are not limited to: • Records of the installation of the patch (e.g., exports from automated patch management tools that provide installation date, verification of BES Cyber System Component software revision, or registry exports that show software has been installed); or • A dated plan showing when and how the vulnerability will be addressed, to include documentation of the actions to be taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch and a timeframe for the completion of these mitigations.

CIP-007-5 Table R2 – Security Patch Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	An example of evidence may include, but is not limited to, records of implementation of mitigations.

R3. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention*. *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].*

M3. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R3 – Malicious Code Prevention* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Deploy method(s) to deter, detect, or prevent malicious code.	An example of evidence may include, but is not limited to, records of the Responsible Entity's performance of these processes (e.g., through traditional antivirus, system hardening, policies, etc.).

CIP-007-5 Table R3 – Malicious Code Prevention			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Mitigate the threat of detected malicious code.	Examples of evidence may include, but are not limited to: • Records of response processes for malicious code detection • Records of the performance of these processes when malicious code is detected.
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	An example of evidence may include, but is not limited to, documentation showing the process used for the update of signatures or patterns.

R4. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]*

M4. Evidence must include each of the documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R4 – Security Event Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	Examples of evidence may include, but are not limited to, a paper or system generated listing of event types for which the BES Cyber System is capable of detecting and, for generated events, is configured to log. This listing must include the required types of events.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	Examples of evidence may include, but are not limited to, paper or system-generated listing of security events that the Responsible Entity determined necessitate alerts, including paper or system generated list showing how alerts are configured.

CIP-007-5 Table R4 – Security Event Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
4.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Examples of evidence may include, but are not limited to, documentation of the event log retention process and paper or system generated reports showing log retention configuration set at 90 days or greater.
4.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Examples of evidence may include, but are not limited to, documentation describing the review, any findings from the review (if any), and dated documentation showing the review occurred.

R5. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M5. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-5 Table 5 – System Access Controls* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	An example of evidence may include, but is not limited to, documentation describing how access is authenticated.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	An example of evidence may include, but is not limited to, a listing of accounts by account types showing the enabled or generic account types in use for the BES Cyber System.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Identify individuals who have authorized access to shared accounts.	An example of evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Change known default passwords, per Cyber Asset capability	Examples of evidence may include, but are not limited to: • Records of a procedure that passwords are changed when new devices are in production; or • Documentation in system manuals or other vendor documents showing default vendor passwords were generated pseudo-randomly and are thereby unique to the device.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.5	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced password parameters, including length and complexity; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.6	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Examples of evidence may include, but are not limited to: • System-generated reports or screen-shots of the system-enforced periodicity of changing passwords; or • Attestations that include a reference to the documented procedures that were followed.

CIP-007-5 Table R5 – System Access Control			
Part	**Applicable Systems**	**Requirements**	**Measures**
5.7	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; 2. PACS; and 3. PCA	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	Examples of evidence may include, but are not limited to: • Documentation of the account-lockout parameters; or • Rules in the alerting configuration showing how the system notified individuals after a determined number of unsuccessful login attempts.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Requirement R1 exists to reduce the attack surface of Cyber Assets by requiring entities to disable known unnecessary ports. The SDT intends for the entity to know what network accessible ("listening") ports and associated services are accessible on their assets and systems, whether they are needed for that Cyber Asset's function, and disable or restrict access to all other ports.

1.1. This requirement is most often accomplished by disabling the corresponding service or program that is listening on the port or configuration settings within the Cyber Asset. It can also be accomplished through using host-based firewalls, TCP Wrappers, or other means on the Cyber Asset to restrict access. Note that the requirement is applicable at the Cyber Asset level. The Cyber Assets are those which comprise the applicable BES Cyber Systems and their associated Cyber Assets. This control is another layer in the defense against network-based attacks, therefore the SDT intends that the control be on the device itself, or positioned inline in a non-bypassable manner. Blocking ports at the ESP border does not substitute for this device level requirement. If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'

1.2. Examples of physical I/O ports include network, serial and USB ports external to the device casing. BES Cyber Systems should exist within a Physical Security Perimeter ~~do~~ in which case the physical I/O ports have protection from unauthorized access, but it may still be possible for accidental use such as connecting a modem, connecting a network cable that

bridges networks, or inserting a USB drive. Ports used for 'console commands' primarily means serial ports on Cyber Assets that provide an administrative interface.

The protection of these ports can be accomplished in several ways including, but not ~~adversely affect existing~~ limited to:

- Disabling all unneeded physical ports within the Cyber Asset's configuration
- Prominent signage, tamper tape, or other means of conveying that the ports should not be used without proper authorization
- Physical port obstruction through removable locks

This is a 'defense in depth' type control and it is acknowledged that there are other layers of control (the PSP for one) that prevent unauthorized personnel from gaining physical access to these ports. Even with physical access, it has been pointed out there are other ways to circumvent the control. This control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense are appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who intends to plug his possibly infected smartphone into an operator console USB port to charge the battery.

Requirement R2:

The SDT's intent of Requirement R2 is to require entities to know, track, and mitigate the known software vulnerabilities associated with their BES Cyber Assets. It is not strictly an "install every security patch" requirement; the main intention is to "be aware of in a timely manner and manage all known vulnerabilities" requirement.

Patch management is required for BES Cyber Systems that are accessible remotely as well as standalone systems. Stand alone systems are vulnerable to intentional or unintentional introduction of malicious code. A sound defense-in-depth security strategy employs additional measures such as physical security, malware prevention software, and software patch management to reduce the introduction of malicious code or the exploit of known vulnerabilities.

One or multiple processes could be utilized. An overall assessment process may exist in a top tier document with lower tier documents establishing the more detailed process followed for individual systems. Lower tier documents could be used to cover BES Cyber System nuances that may occur at the system level.

2.1. The Responsible Entity is to have a patch management program that covers tracking, evaluating, and installing cyber security ~~controls~~patches. The requirement applies to patches only, which are fixes released to handle a specific vulnerability in a hardware or software product. The requirement covers only patches that involve cyber security fixes and does not cover patches that are purely functionality related with no cyber security impact. Tracking

involves processes for notification of the availability of new cyber security patches for the Cyber Assets. Documenting the patch source in the tracking portion of the process is required to determine when the assessment timeframe clock starts. This requirement handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system. The source can take many forms. The National Vulnerability Database, Operating System vendors, or Control System vendors could all be sources to monitor for release of security related patches, hotfixes, and/or updates. 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. The identification of these sources is intended to be performed once unless software is changed or added to the Cyber Asset's baseline.

2.2. Responsible Entities are to perform an assessment of security related patches within 35 days of release from their monitored source. An assessment should consist of determination of the applicability of each patch to the entity's specific environment and systems. Applicability determination is based primarily on whether the patch applies to a specific software or hardware component that the entity does have installed in an applicable Cyber Asset. A patch that applies to a service or component that is not installed in the entity's environment is not applicable. If the patch is determined to be non-applicable, that is documented with the reasons why and the entity is compliant. If the patch is applicable, the assessment can include a determination of the risk involved, how the vulnerability can be remediated, the urgency and timeframe of the remediation, and the steps the entity has previously taken or will take. Considerable care must be taken in applying security related patches, hotfixes, and/or updates or applying compensating measures to BES Cyber System or BES Cyber Assets that are no longer supported by vendors. It is possible security patches, hotfixes, and updates may reduce the reliability of the system, and entities should take this into account when determining the type of mitigation to apply. The Responsible Entities can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as a source. The DHS document "Recommended Practice for Patch Management of Control Systems" provides guidance on an evaluative process. It uses severity levels determined using the Common Vulnerability Scoring System Version 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.

When documenting the remediation plan measures it may not be necessary to document them on a one to one basis. The remediation plan measures may be cumulative. A measure to address a software vulnerability may involve disabling a particular service. That same service may be exploited through other software vulnerabilities. Therefore disabling the single service has addressed multiple patched vulnerabilities.

2.3. The requirement handles the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity either installs the patch or documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. There are times when it is in the best interest of reliability to not install a patch, and the entity can

document what they have done to mitigate the vulnerability. For those security related patches that are determined to be applicable, the Responsible Entity must within 35 days either install the patch, create a dated mitigation plan which will outline the actions to be taken or those that have already been taken by the Responsible Entity to mitigate the vulnerabilities addressed by the security patch, or revise an existing mitigation plan. Timeframes do not have to be designated as a particular calendar day but can have event designations such as "at next scheduled outage of at least two days duration." "Mitigation plans" in the standard refers to internal documents and are not to be confused with plans that are submitted to Regional Entities in response to violations.

2.4. The entity has been notified of, has assessed, and has developed a plan to remediate the known risk and that plan must be implemented. Remediation plans that only include steps that have been previously taken are considered implemented upon completion of the documentation. Remediation plans that have steps to be taken to remediate the vulnerability must be implemented by the timeframe the entity documented in their plan. There is no maximum timeframe in this requirement as patching and other system changes carries its own risk to the availability and integrity of the systems and may require waiting until a planned outage. In periods of high demand or threatening weather, changes to systems may be curtailed or denied due to the risk to reliability.

Requirement R3:

3.1. Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, portable storage media policies, Intrusion Detection/Prevention (IDS/IPS) solutions, etc. If an entity has numerous BES Cyber Systems or Cyber Assets that are of identical architecture, they may provide one process that describes how all the like Cyber Assets are covered. If a specific Cyber Asset has no updateable software and its executing code cannot be altered, then that Cyber Asset is considered to have its own internal method of deterring malicious code.

3.2. When malicious code is detected on a Cyber Asset within the applicability of this requirement, the threat posed by that code must be mitigated. In situations where traditional antivirus products are used, they may be configured to automatically remove or quarantine the malicious code. In white-listing situations, the white-listing tool itself can mitigate the threat as it will not allow the code to execute, however steps should still be taken to remove the malicious code from the Cyber Asset. In some instances, it may be in the best interest of reliability to not immediately remove or quarantine the malicious code, such as when availability of the system may be jeopardized by removal while operating and a rebuild of the system needs to be scheduled. In that case, monitoring may be increased and steps taken to insure the malicious code cannot communicate with other systems. In some instances the entity may be working with law enforcement or other governmental entities to closely monitor the code and track the perpetrator(s). For these reasons, there is no maximum timeframe or

method prescribed for the removal of the malicious code, but the requirement is to mitigate the threat posed by the now identified malicious code.

3.3. In instances where malware detection technologies depend on signatures or patterns of known attacks, the effectiveness of these tools against evolving threats is tied to the ability to keep these signatures and patterns updated in a timely manner. The entity is to have a documented process that includes the testing and installation of signature or pattern updates. In a BES Cyber System, there may be some Cyber Assets that would benefit from the more timely installation of the updates where availability of that Cyber Asset would not jeopardize the availability of the BES Cyber System's ability to perform its function. For example, some HMI workstations where portable media is utilized may benefit from having the very latest updates at all times with minimal testing. Other Cyber Assets should have any updates thoroughly tested before implementation where the result of a 'false positive' could harm the availability of the BES Cyber System. The testing should not negatively impact the reliability of the BES. The testing should be focused on the update itself and if it will have an adverse impact on the BES Cyber System. Testing in no way implies that the entity is testing to ensure that malware is indeed detected by introducing malware into the environment. It is strictly focused on ensuring that the update does not negatively impact the BES Cyber System before those updates are placed into production.

Requirement R4:

Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring.

4.1. In a complex computing environment and faced with dynamic threats and vulnerabilities, it is not practical within the standard to enumerate all security-related events necessary to support the activities for alerting and incident response. Rather, the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.

Specific security events already required in Version 4 of the CIP Standards carry forward in this version. This includes access attempts at the Electronic Access Points, if any have been identified for a BES Cyber Systems. Examples of access attempts include: (i) blocked network access attempts, (ii) successful and unsuccessful remote user access attempts, (iii) blocked network access attempts from a remote VPN, and (iv) successful network access attempts or network flow information.

User access and activity events include those events generated by Cyber Assets within the Electronic Security Perimeter that have access control capability. These types of events include: (i) successful and unsuccessful authentication, (ii) account management, (iii) object access, and (iv) processes started and stopped.

It is not the intent of the SDT that if a device cannot log a particular event that a TFE must be generated. The SDT's intent is that if any of the items in the bulleted list (for example, user logouts) can be logged by the device then the entity must log that item. If the device does not have the capability of logging that event, the entity remains compliant.

4.2. Real-time alerting allows the cyber system to automatically communicate events of significance to designated responders. This involves configuration of a communication mechanism and log analysis rules. Alerts can be configured in the form of an email, text message, or system display and alarming. The log analysis rules can exist as part of the

operating system, specific application or a centralized security event monitoring system. On one end, a real-time alert could consist of a set point on an RTU for a login failure, and on the other end, a security event monitoring system could provide multiple alerting communications options triggered on any number of complex log correlation rules.

The events triggering a real-time alert may change from day to day as system administrators and incident responders better understand the types of events that might be indications of a cyber-security incident. Configuration of alerts also must balance the need for responders to know an event occurred with the potential inundation of insignificant alerts. The following list includes examples of events a Responsible Entity should consider in configuring real-time alerts:

- Detected known or potential malware or malicious activity
- Failure of security event logging mechanisms
- Login failures for critical accounts
- Interactive login of system accounts
- Enabling of accounts
- Newly provisioned accounts
- System administration or change tasks by an unauthorized user
- Authentication attempts on certain accounts during non-business hours
- Unauthorized configuration changes
- Insertion of removable media in violation of a policy

4.3 Logs that are created under Part 4.1 are to be retained on the applicable Cyber Assets or BES Cyber Systems for at least 90 days. This is different than the evidence retention period called for in the CIP standards used to prove historical compliance. For such audit 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.~~, the entity should maintain evidence that shows that 90 days were kept historically. One example would be records of disposition of event logs beyond 90 days up to the evidence retention period.

~~o 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.~~

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

~~o The Responsible Entity shall document test results.~~

~~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.~~

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

- 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).
- 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.

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 shall **4.4.** Reviewing logs at least every 15 days (approximately every two weeks) can consist of analyzing a summarization or sampling of logged events. NIST SP800-92 provides a lot of guidance in periodic log analysis. If a centralized security event monitoring system is used, log analysis can be performed top-down starting with a review of trends from summary reports. The log review can also be an extension of the exercise in identifying those events needing real-time alerts by analyzing events that are not fully understood or could possibly inundate the real-time alerting.

Requirement R5:

Account types referenced in this guidance typically include:

- Shared user account: An account used by multiple users for normal business functions by employees or contractors. Usually on a device that does not support Individual User Accounts.
- Individual user account: An account used by a single user.
- Administrative account: An account with elevated privileges for performing administrative or other specialized functions. These can be individual or shared accounts.
- System account: Accounts used to run services on a system (web, DNS, mail etc). No users have access to these accounts.
- Application account: A specific system account, with rights granted at the application level often used for access into a Database.
- Guest account: An individual user account not typically used for normal business functions by employees or contractors and not associated with a specific user. May or may not be shared by multiple users.
- Remote access account: An individual user account only used for obtaining Interactive Remote Access to the BES Cyber System.
- Generic account: A group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type.

5.1 Reference the Requirement's rationale.

5.2 Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level.

5.3 Entities may choose to identify individuals with access to shared accounts through the access authorization and provisioning process, in which case the individual authorization records suffice to meet this Requirement Part. Alternatively, entities may choose to maintain a separate listing for shared accounts. Either form of evidence achieves the end result of maintaining control of shared accounts.

5.4. Default passwords can be commonly published in vendor documentation that is readily available to all customers using that type of equipment and possibly published online.

The requirement option to have unique password addresses cases where the Cyber Asset generates or has assigned pseudo-random default passwords at the time of production or installation. In these cases, the default password does not have to change because the system or manufacturer created it specific to the Cyber Asset.

5.5. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Technical or procedural enforcement of password parameters are required where passwords are the only credential used to authenticate individuals. Technical enforcement of the password parameters means a Cyber Asset verifies an individually selected password meets the required parameters before allowing the account to authenticate with the selected password. Technical enforcement should be used in most cases when the authenticating Cyber Asset supports enforcing password parameters. Likewise, procedural enforcement means requiring the password parameters through procedures. Individuals choosing the passwords have the obligation of ensuring the password meets the required parameters.

Password complexity refers to the policy set by a Cyber Asset to require passwords to have one or more of the following types of characters: (1) lowercase alphabetic, (2) uppercase alphabetic, (3) numeric, and (4) non-alphanumeric or “special” characters (e.g. #, $, @, &), in various combinations.

5.6 Technical or procedural enforcement of password change obligations are required where passwords are the only credential used to authenticate individuals. Technical enforcement of password change obligations means the Cyber Asset requires a password change after a specified timeframe prior to allowing access. In this case, the password is not required to change by the specified time as long as the Cyber Asset enforces the password change after the next successful authentication of the account. Procedural enforcement means manually changing passwords used for interactive user access after a specified timeframe.

5.7 Configuring an account lockout policy or alerting after a certain number of failed authentication attempts serves to prevent unauthorized access through an online password guessing attack. The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate. It should also be set low enough to account for online password attacks occurring over an extended period of time. This threshold may be tailored to the operating environment over time to avoid unnecessary account lockouts.

Entities should take caution when configuring account lockout to avoid locking out accounts necessary for the BES Cyber System to perform a BES reliability task. In such cases, entities should configure authentication failure alerting.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Summary of Changes: Changed the 'needed for normal or emergency operations' to those ports that are needed. Physical I/O ports were added in response to a FERC order. The unneeded physical ports in Control Centers (which are the highest risk, most impactful areas) should be protected as well.

Reference to prior version: (Part 1.1) CIP-007-4, R2.1 and R2.2

Change Rationale: (Part 1.1)

The requirement focuses on the entity knowing and only allowing those ports that are necessary. The additional classification of 'normal or emergency' added no value and has been removed.

Reference to prior version: (Part 1.2) New

Change Rationale: (Part 1.2)

On March 18, 2010, FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.

Rationale for R2:

Security patch management is a proactive way of monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner to gain control of or render a BES Cyber Asset or BES Cyber System inoperable.

The remediation plan can be updated as necessary to maintain the reliability of the BES, including an explanation of any rescheduling of the remediation actions.

1.1. **Summary of Changes:** The existing wordings of CIP-007, Requirements R3, R3.1, and R3.2, were separated into individual line items to provide more granularity. The documentation of a source(s) to monitor for release of security related patches, hot fixes, and/or updates for BES Cyber System or BES Cyber Assets was added to provide context as to when the "release" date was. The current wording stated "document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades" and there has been confusion as to what constitutes the availability date. Due to issues that may occur regarding Control System vendor license and service agreements, flexibility must be given to Responsible Entities to define what sources are being monitored for BES Cyber Assets.

- 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.

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).

- 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.
- 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.

Account Management — The Responsible Entity shall**Reference to prior version:** (Part 2.1) CIP-007, R3

Change Rationale: (Part 2.1)

The requirement is brought forward from previous CIP versions with the addition of defining the source(s) that a Responsible Entity monitors for the release of security related patches. Documenting the source is used to determine when the assessment timeframe clock starts. This requirement also handles the situation where security patches can come from an original source (such as an operating system vendor), but must be approved or certified by another source (such as a control system vendor) before they can be assessed and applied in order to not jeopardize the availability or integrity of the control system.

Reference to prior version: (Part 2.2) CIP-007, R3.1

Change Rationale: (Part 2.2)

Similar to the current wording but added "from the source or sources identified in 2.1" to clarify the 35-day time frame.

Reference to prior version: (Part 2.3) CIP-007, R3.2

Change Rationale: (Part 2.3)

The requirement has been changed to handle the situations where it is more of a reliability risk to patch a running system than the vulnerability presents. In all cases, the entity documents (either through the creation of a new or update of an existing mitigation plan) what they are going to do to mitigate the vulnerability and when they are going to do so. The mitigation plan may, and in many cases will, consist of installing the patch. However, there are times when it is in the best interest of reliability to not install a patch, and the entity can document what they have done to mitigate the vulnerability.

Reference to prior version: (Part 2.4) CIP-007, R3.2

Change Rationale: (Part 2.4)

Similar to the current wording but added that the plan must be implemented within the timeframe specified in the plan, or in a revised plan as approved by the CIP Senior Manager or delegate.

Rationale for R3:

Malicious code prevention has the purpose of limiting and detecting the addition of malicious code onto the applicable Cyber Assets of a BES Cyber System. Malicious code (viruses, worms, botnets, targeted code such as Stuxnet, etc.) may compromise the availability or integrity of the BES Cyber System.

Summary of Changes: In prior versions, this requirement has arguably been the single greatest generator of TFEs as it prescribed a particular technology to be used on every CCA regardless of that asset's susceptibility or capability to use that technology. As the scope of Cyber Assets in scope of these standards expands to more field assets, this issue will grow exponentially. The drafting team is taking the approach of making this requirement a competency based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every Cyber Asset. The BES Cyber System is the object of protection.

Beginning in Paragraphs 619-622 of FERC Order No. 706, and in particular Paragraph 621, FERC agrees that the standard "does not need to prescribe a single method…However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance…"

In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.

Reference to prior version: (Part 3.1) CIP-007-4, R4; CIP-007-4, R4.1

Change Rationale: (Part 3.1)

See the Summary of Changes. FERC Order No. 706, Paragraph 621, states the standards development process should decide to what degree to protect BES Cyber Systems from personnel introducing malicious software.

Reference to prior version: (Part 3.2) *CIP-007-4, R4; CIP-007-4, R4.1*
Change Rationale: (Part 3.2)

See the Summary of Changes.

Reference to prior version: (Part 3.3) CIP-007-4, R4; CIP-007-4, R4.2

Change Rationale: (Part 3.3)

Requirement essentially unchanged from previous versions; updated to refer to previous parts of the requirement table.

Rationale for R4:

Rationale for R4: Security event monitoring has the purpose of detecting unauthorized access, reconnaissance and other malicious activity on BES Cyber Systems, and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the detection of an incident and (2) useful evidence in the investigation of an incident. The retention of security-related logs is intended to support post-event data analysis.

Audit processing failures are not penalized in this requirement. Instead, the requirement specifies processes which must be in place to monitor for and notify personnel of audit processing failures.

Summary of Changes: Beginning in Paragraph 525 and also Paragraph 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis. This requirement combines CIP-005-4, R5 and CIP-007-4, R6 and addresses both directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms “security event” and “monitor.”

The term “security event” or “events related to cyber security” is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach similar to NIST 800-53 and requires the entity to define the security events relevant to the System. There are a few events explicitly listed that if a Cyber Asset or BES Cyber System can log, then it must log.

In addition, this requirement sets up parameters for the monitoring and reviewing of processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order No. 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review.

Reference to prior version: (Part 4.1) CIP-005-4, R3; CIP-007-4, R5, R5.1.2, R6.1, and R6.3

Change Rationale: (Part 4.1)

This requirement is derived from NIST 800-53 version 3 AU-2, which requires organizations to determine system events to audit for incident response purposes. The industry expressed

confusion in the term "system events related to cyber security" from informal comments received on CIP-011. Access logs from the ESP as required in CIP-005-4 Requirement R3 and user access and activity logs as required in CIP-007-5 Requirement R5 are also included here.

Reference to prior version: (Part 4.2) CIP-005-4, R3.2; CIP-007-4, R6.2

Change Rationale: (Part 4.2)

This requirement is derived from alerting requirements in CIP-005-4, Requirement R3.2 and CIP-007-4, Requirement R6.2 in addition to NIST 800-53 version 3 AU-6. Previous CIP Standards required alerting on unauthorized access attempts and detected Cyber Security Incidents, which can be vast and difficult to determine from day to day. Changes to this requirement allow the entity to determine events that necessitate a response.

Reference to prior version: (Part 4.3) CIP-005-4, R3.2; CIP-007-4, R6.4

Change Rationale: (Part 4.3)

No substantive change.

Reference to prior version: (Part 4.4) CIP-005-4, R3.2; CIP-007-4, R6.5

Change Rationale: (Part 4.4)

Beginning in Paragraph 525 and also 628 of the FERC Order No. 706, the Commission directs a manual review of security event logs on a more periodic basis and suggests a weekly review. The Order acknowledges it is rarely feasible to review all system logs. Indeed, log review is a dynamic process that should improve over time and with additional threat information. Changes to this requirement allow for an approximately biweekly summary or sampling review of logs.

Rationale for R5:

To help ensure that no authorized individual can gain electronic access to a BES Cyber System until the individual has been authenticated, i.e., until the individual's logon credentials have been validated. Requirement R5 also seeks to reduce the risk that static passwords, where used as authenticators, may be compromised.

Requirement Part 5.1 ensures the BES Cyber System or Cyber Asset authenticates individuals that can modify configuration information. This requirement addresses the configuration of authentication. The authorization of individuals is addressed elsewhere in the CIP Cyber Security Standards. Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, etc.). For devices that cannot technically or for operational reasons perform authentication, an entity may demonstrate all interactive user access paths, both remote and local, are configured for authentication. Physical security suffices for local access configuration if the physical security can record who is in the Physical Security Perimeter and at what time.

Requirement Part 5.2 addresses default and other generic account types. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The Requirement Part avoids prescribing an action to address these accounts because the most

effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Requirement Part 5.3 addresses identification of individuals with access to shared accounts. This Requirement Part has the objective of mitigating the risk of unauthorized access through shared accounts. This differs from other CIP Cyber Security Standards Requirements to authorize access. An entity can authorize access and still not know who has access to a shared account. Failure to identify individuals with access to shared accounts would make it difficult to revoke access when it is no longer needed. The term "authorized" is used in the requirement to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement.

Requirement 5.4 addresses default passwords. Changing default passwords closes an easily exploitable vulnerability in many systems and applications. Pseudo-randomly system generated passwords are not considered default passwords.

For password-based user authentication, using strong passwords and changing them periodically helps mitigate the risk of successful password cracking attacks and the risk of accidental password disclosure to unauthorized individuals. In these requirements, the drafting team considered multiple approaches to ensuring this requirement was both effective and flexible enough to allow Responsible Entities to make good security decisions. One of the approaches considered involved requiring minimum password entropy, but the calculation for true information entropy is more highly complex and makes several assumptions in the passwords users choose. Users can pick poor passwords well below the calculated minimum entropy.

The drafting team also chose to not require technical feasibility exceptions for devices that cannot meet the length and complexity requirements in password parameters. The objective of this requirement is to apply a measurable password policy to deter password cracking attempts, and replacing devices to achieve a specified password policy does not meet this objective. At the same time, this requirement has been strengthened to require account lockout or alerting for failed login attempts, which in many instances better meets the requirement objective.

The requirement to change passwords exists to address password cracking attempts if an encrypted password were somehow attained and also to refresh passwords which may have been accidentally disclosed over time. The requirement permits the entity to specify the periodicity of change to accomplish this objective. Specifically, the drafting team felt determining the appropriate periodicity based on a number of factors is more effective than specifying the period for every BES Cyber System in the Standard. In general, passwords for user authentication should be changed at least annually. The periodicity may increase in some cases. For example, application passwords that are long and pseudo-randomly generated could have a very long periodicity. Also, passwords used only as a weak form of application authentication, such as accessing the configuration of a relay may only need to be changed as part of regularly scheduled maintenance.

The Cyber Asset should automatically enforce the password policy for individual user accounts. However, for shared accounts in which no mechanism exists to enforce password policies, the Responsible Entity can enforce the password policy procedurally and through internal assessment and audit.

Requirement Part 5.7 assists in preventing online password attacks by limiting the number of guesses an attacker can make. This requirement allows either limiting the number of failed authentication attempts or alerting after a defined number of failed authentication attempts. Entities should take caution in choosing to limit the number of failed authentication attempts for all accounts because this would allow the possibility for a denial of service attack on the BES Cyber System.

Summary of Changes (From R5):

CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. For example, many have interpreted the password for tokens or biometrics must satisfy this policy and in some cases prevents the use of this stronger authentication. Also, longer passwords may preclude the use of strict complexity requirements. The password requirements have been changed to allow the entity to specify the most effective password parameters based on the impact of the BES Cyber System, the way passwords are used, and the significance of passwords in restricting access to the system. The SDT believes these changes strengthen the authentication mechanism by requiring entities to look at the most effective use of passwords in their environment. Otherwise, prescribing a strict password policy has the potential to limit the effectiveness of security mechanisms and preclude better mechanisms in the future.

Reference to prior version: (Part 5.1) CIP-007-4, R5

Change Rationale: (Part 5.1)

The requirement to enforce authentication for all user access is included here. The requirement to establish, implement, and document *controls is included in this introductory requirement. The requirement to have* technical and procedural controls ~~that enforce access authentication of, and accountability for, all user activity, and~~ *was removed because technical controls suffice when procedural documentation is already required. The phrase "*that minimize the risk of unauthorized ~~system access.~~*access" was removed and more appropriately captured in the rationale statement.*

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

~~The Responsible Entity shall implement a policy~~ **Reference to prior version:** (Part 5.2) CIP-007-4, R5.2 and R5.2.1

Change Rationale: (Part 5.2)

1.2. *CIP-007-4 requires entities to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.account privileges. The requirement to minimize account privileges has been removed because the implementation of such a policy is difficult to measure at best.*

Reference to prior version: (Part 5.3) CIP-007-4, R5.2.2

Change Rationale: (Part 5.3)

No significant changes. Added "authorized" access to make clear that individuals storing, losing or inappropriately sharing a password is not a violation of this requirement.

Reference to prior version: (Part 5.4) CIP-007-4, R5.2.1

Change Rationale: (Part 5.4)

The policy shall include requirement for the "removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, " has been removed and incorporated into guidance for acceptable use of account types. This was removed because those actions are not appropriate on all account types. Added the option of having unique default passwords shall beto permit cases where a system may have generated a default password or a hard-coded uniquely generated default password was manufactured with the BES Cyber System.

Reference to prior version: (Part 5.5) CIP-007-4, R5.3

Change Rationale: (Part 5.5)

1.2.1. *CIP-007-4, Requirement R5.3 requires the use of passwords and specifies a specific policy of six characters or more with a combination of alpha-numeric and special characters. The level of detail in these requirements can restrict more effective security measures. The password requirements have been changed prior to putting any system into service.to permit the maximum allowed by the device in cases where the password parameters could otherwise not achieve a stricter policy. This change still achieves the requirement objective to minimize the risk of unauthorized disclosure of password credentials while recognizing password parameters alone do not achieve this. The drafting team felt allowing the Responsible Entity the flexibility of applying the strictest password policy allowed by a device outweighed the need to track a relatively minimally effective control through the TFE process.*

- The Responsible Entity shall identify those individuals with access to shared accounts.
- 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).

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

- Each password shall be a minimum of six characters.

- Each password shall consist of a combination of alpha, numeric, and "special" characters.
- Each password shall be changed at least annually, or more frequently based on risk.

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 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.
- The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
- 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.
- The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
- The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

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.

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

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:

- A document identifying the vulnerability assessment process;
- A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
- A review of controls for default accounts; and,
- 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.

- 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

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

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

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

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

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

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

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.

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.

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 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).
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	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.

		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	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.

			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	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),	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).

			~~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).~~	~~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~~	~~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.~~

			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.~~

Reference to prior version: (Part 5.6) CIP-007-4, R5.3.3

Change Rationale: (Part 5.6)

**This was originally Requirement R5.5.3, but moved to add "external routable connectivity" to medium impact in response to comments. This requirement is limited in scope because the risk to performing an online password attack is lessened by its lack of external routable connectivity. Frequently changing passwords at field assets can entail significant effort with minimal risk reduction.*

Reference to prior version: (Part 5.7) *New Requirement*

Change Rationale: (Part 5.7)

Minimizing the number of unsuccessful login attempts significantly reduces the risk of live password cracking attempts. This is a more effective control in live password attacks than password parameters.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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 ~~**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	12/16/09	Updated version ~~numbers~~number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
~~3~~4	1/24/11~~12/16/09~~	Approved by the NERC Board of Trustees.	Update
~~4~~5	~~Board approved 01/24/2011~~11/26/12	Adopted by the NERC Board of Trustees.~~Update version number from "3" to "4"~~	Modified to coordinate with other CIP standards and to revise format to use RBS Template.~~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: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-008-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training

program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

R2. Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with	The Responsible Entity has not updated the	The Responsible Entity has neither	The Responsible Entity has neither

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR	documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the	documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

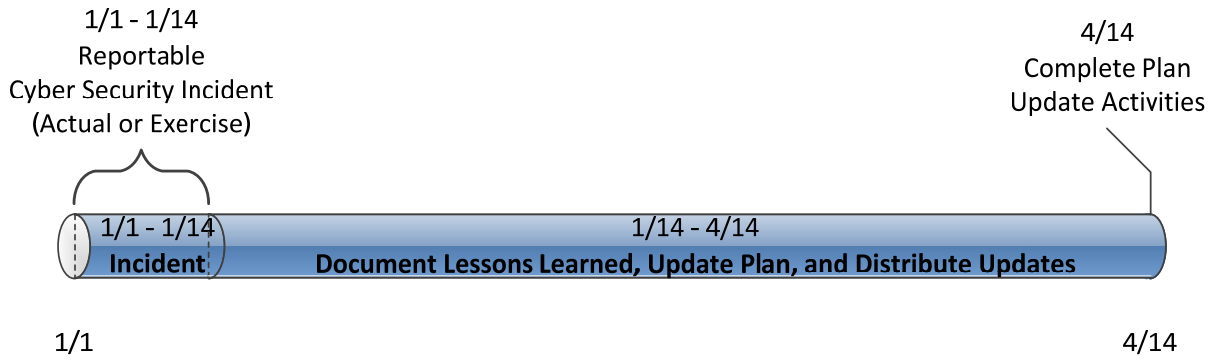


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

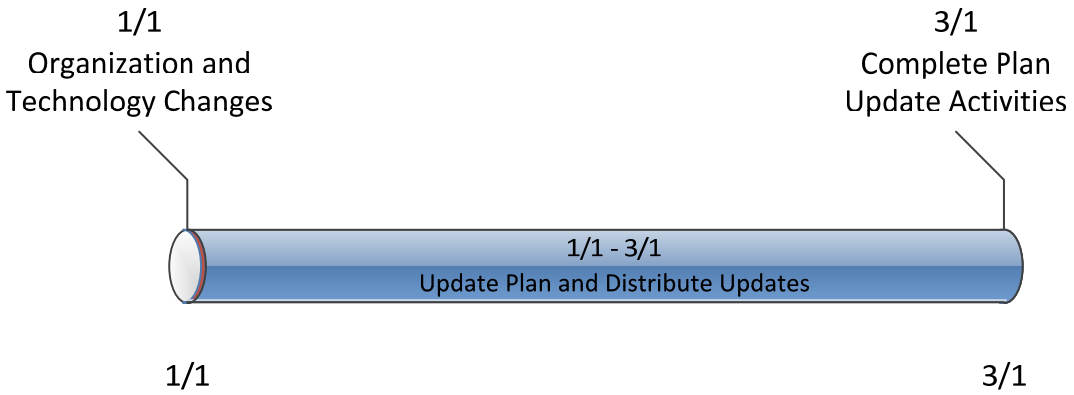


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)
Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the

plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	

4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-45

3. Purpose: Standard CIP-008-4 ensuresTo mitigate the identification, classification, response, and reportingrisk to the reliable operation of the BES as the result of a Cyber Security Incidents related to Critical Cyber Assets. Incident by specifying incident response requirements.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard CIP-008-4 should be read as part of a .

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

3.4.1.2.4 Each Cranking Path and group of standards numbered Standards CIP-002-4 through CIP-009-4. Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4. Applicability

4.1. Within the text of Standard CIP-008-4, "Responsible Entity" shall mean:

4.1.3 ~~Reliability~~**Generator Operator**

4.1.4 Generator Owner

~~**4.1.1 Interchange** **Coordinator.**~~

~~**4.1.2 Balancing Authority.**~~

~~**4.1.3**~~**4.1.5 or Interchange Authority**~~.~~

~~**4.1.4 Transmission Service Provider.**~~

4.1.6 Reliability Coordinator

~~**4.1.5**~~**4.1.7 Transmission** ~~Owner.~~**Operator**

~~**4.1.6 Transmission** Operator.~~

~~**4.1.7**~~**4.1.8** ~~Generator~~ **Owner**~~.~~

~~**4.1.8 Generator Operator.**~~

~~**4.1.9 Load Serving Entity.**~~

~~**4.1.10 NERC.**~~

~~**4.1.11 Regional Entity.**~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~**4.2.**~~**4.2.3 Exemptions:** The following are exempt from Standard CIP-008-~~4:~~5:

~~**4.2.1**~~**4.2.3.1** Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~**4.2.2**~~**4.2.3.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~**4.2.3**~~**4.2.3.3** ~~In nuclear plants, the~~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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

~~**4.2.4**~~**4.2.3.5** Responsible Entities that~~, in compliance with Standard CIP-002-4,~~ identify that they have no ~~Critical~~BES Cyber ~~Assets~~Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective ~~Date:~~ The ~~Dates:~~

1. **24 Months Minimum** – CIP-008-5 shall become effective on the later of July 1, 2015, or the first ~~day of the eighth~~ calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory ~~approvals have been received (or the Reliability Standard otherwise becomes effective~~ approval.

~~**5.**~~ 2. In those jurisdictions where no regulatory approval is required, CIP-008-5 shall become effective on the first day of the ninth calendar quarter ~~after BOT adoption in those jurisdictions where regulatory approval is not required).~~following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

B. Requirements and Measures

~~Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a~~

R1. Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 –* *Cyber Security Incident* ~~response plan and implement the plan in response to Cyber Security Incidents. The~~ *Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].*

~~R1.~~M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable requirement parts in *CIP-008-5 Table R1 –* *Cyber Security Incident* ~~response plan shall address, at a minimum, the following:~~*Response Plan Specifications*.

~~**1.1.** Procedures to characterize and classify events as reportable Cyber Security Incidents.~~

~~**1.2.** Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.~~

~~**1.3.** 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.~~

~~**1.4.** Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.~~

~~**1.5.** Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.~~

~~**1.6.** 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.~~

~~**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.~~

~~C. Measures~~

~~The~~

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to identify, classify, and respond to Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation of Cyber Security Incident response plan(s) that include the process to identify, classify, and respond to Cyber Security Incidents.
1.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated documentation of Cyber Security Incident response plan(s) that provide guidance or thresholds for determining which Cyber Security Incidents are also Reportable Cyber Security Incidents and documentation of initial notices to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
1.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	The roles and responsibilities of Cyber Security Incident response groups or individuals.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that define roles and responsibilities (e.g., monitoring, reporting, initiating, documenting, etc.) of Cyber Security Incident response groups or individuals.

CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Incident handling procedures for Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated Cyber Security Incident response process(es) or procedure(s) that address incident handling (e.g., containment, eradication, recovery/incident resolution).

~~M1.~~**R2.** Each Responsible Entity shall ~~make available~~implement each of its documented Cyber Security Incident response ~~plan as indicated in Requirement R1 and documentation of the review, updating, and testing of the plan.~~plans to collectively include each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].*

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

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.
2.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Examples of evidence may include, but are not limited to, incident reports, logs, and notes that were kept during the incident response process, and follow-up documentation that describes deviations taken from the plan during the incident or exercise.

CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Retain records related to Reportable Cyber Security Incidents.	An example of evidence may include, but is not limited to, dated documentation, such as security logs, police reports, emails, response forms or checklists, forensic analysis results, restoration records, and post-incident review notes related to Reportable Cyber Security Incidents.

R3. Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Evidence must include, but is not limited to, documentation that collectively demonstrates maintenance of each Cyber Security Incident response plan according to the applicable requirement parts in *CIP-008-5 Table R3 – Cyber Security Incident.*

CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of post incident(s) review meeting notes or follow-up report showing lessons learned associated with the Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response or dated documentation stating there were no lessons learned; 2. Dated and revised Cyber Security Incident response plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.
CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication			

Part	Applicable Systems	Requirements	Measures
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan: 3.2.1. Update the Cyber Security Incident response plan(s); and 3.2.2. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	An example of evidence may include, but is not limited to: 1. Dated and revised Cyber Security Incident response plan with changes to the roles or responsibilities, responders or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

~~D.~~C. 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~~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,~~ ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by ~~the ERO and~~ FERC or other applicable governmental ~~authorities~~authority shall serve as the ~~Compliance Enforcement Authority~~CEA.

1.2. ~~For the ERO, a third-party monitor without vested interest~~**Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in ~~the outcome~~this standard for ~~the ERO~~three calendar years.
- ~~**1.2.4**~~ If a Responsible Entity is found non-compliant, it shall ~~serve as~~keep information related to the non-compliance until mitigation is complete and approved or for the ~~Compliance Enforcement Authority~~time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and ~~Enforcement~~Assessment Processes:

- Compliance ~~Audits~~Audit
- Self-~~Certifications~~Certification
- Spot Checking
- Compliance ~~Violation Investigations~~Investigation
- Self-Reporting

~~Complaints~~

~~**1.4. Data Retention**~~

~~1.4.1 The Responsible Entity shall keep documentation other than that required for reportable Cyber Security Incidents as specified in Standard CIP-008-4 for 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.~~

- Complaint

~~1.5.~~1.4. **Additional Compliance Information:**

~~1.5.1 The Responsible Entity may not take exception in its cyber security policies to the creation of a Cyber Security Incident response plan.~~

~~1.5.2 The Responsible Entity may not take exception in its cyber security policies to reporting Cyber Security Incidents to the ES ISAC.~~

~~2. Violation Severity Levels~~

- None

2. Table of Compliance Elements

R # 2.	Time Horizon	VRF VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	Long Term Planning	LOWER Lower	N/A	The Responsible Entity has developed but not maintained a Cyber Security Incident response plan.N/A	The Responsible Entity has developed athe Cyber Security Incident response plan(s), but the plan does not address oneinclude the roles and responsibilities of Cyber Security Incident response groups or more of the subrequirements R1.individuals. (1 through.3) R1.6.OR The Responsible Entity has developed the Cyber Security Incident response	The Responsible Entity has not developed a Cyber Security Incident response plan orwith one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has not implemented the plan in response to developed a Cyber Security Incident. response plan, but the plan does not include one or more processes to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
2.		~~VRF~~	Lower VSL	Moderate VSL	High VSL	Severe VSL
					plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
~~R1.1.~~		~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.2.~~ R	**Operations**	~~LOWER~~**Lowe**	~~N/A~~The Responsible Entity has not tested	~~N/A~~The Responsible Entity has not tested	~~N/A~~The Responsible Entity has not tested	~~N/A~~The Responsible Entity has not tested

2	**Planning** **Real-time Operations**	r	the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

~~R1.3.~~		~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.4.~~		~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.5.~~		~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~
~~R1.6.~~		~~LOWER~~	~~N/A~~	~~N/A~~	~~N/A~~	~~N/A~~

~~R2~~R3	**Operations Assessment**	~~LOWER~~ **Lower**	The Responsible Entity has ~~kept relevant documentation related to~~ not notified each person or group	The Responsible Entity has ~~kept relevant documentation related to~~ not updated the Cyber Security ~~Incidents reportable per Requirement R1.1~~	The Responsible Entity has ~~kept relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for~~ neither documented	The Responsible Entity has ~~not kept relevant documentation related~~ neither documented lessons

			with a defined role in the Cyber Security Incidents reportable per Requirement R1.1 for twoIncident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than three120 calendar years.days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	forIncident response plan based on any documented lessons learned within 90 and less than two120 calendar yearsdays of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response	lessons learned nor documented the absence of any lessons learned within 90 and less than one120 calendar yeardays of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group	learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incidents reportable per Requirement R1Incident. (3.1.1)

				plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

~~E.~~D. Regional Variances

None ~~identified~~.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a Cyber Security Incident response plan:

- Department of Homeland Security, Control Systems Security Program, *Developing an Industrial Control Systems Cyber Security Incident Response Capability*, 2009, online at http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf
- National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61 revision 1, March 2008, online at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. It is helpful to distinguish Reportable Cyber Security Incidents as one resulting in a necessary response action. A response action can fall into one of two categories: Necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions to avoid any persistent damage or adverse effects, which include the activation of redundant systems, should be designated as necessary.

The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This addition is in response to the directive addressing this issue in FERC Order No. 706, paragraphs 673 and 676, to report within one hour (at least preliminarily). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report.

Requirement R2:

Requirement R2 ensures entities periodically test the Cyber Security Incident response plan. This includes the requirement in Part 2.2 to ensure the plan is actually used when testing. The testing requirements are specifically for *Reportable Cyber Security Incidents*.

Entities may use an actual response to a *Reportable Cyber Security Incident* as a substitute for exercising the plan annually. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or full operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. Table top exercises (TTX) can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

In addition to the requirements to implement the response plan, Part 2.3 specifies entities must retain relevant records for *Reportable Cyber Security Incidents*. There are several examples of specific types of evidence listed in the measure. Entities should refer to their handling procedures to determine the types of evidence to retain and how to transport and store the evidence. For further information in retaining incident records, refer to the NIST Guide to Integrating Forensic Techniques into Incident Response (SP800-86). The NIST guideline includes a section (Section 3.1.2) on acquiring data when performing forensics.

Requirement R3:

This requirement ensures entities maintain Cyber Security Incident response plans. There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.1 and (2) organizational or technology changes from Part 3.2.

The documentation of lessons learned from Part 3.1 is associated with each Reportable Cyber Security Incident and involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the incident in recognition that complex incidents on complex systems can take a few days or weeks to complete response

activities. The process of conducting lessons learned can involve the response team discussing the incident to determine gaps or areas of improvement within the plan. Any documented deviations from the plan from Part 2.2 can serve as input to the lessons learned. It is possible to have a *Reportable Cyber Security Incident* without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the *Reportable Cyber Security Incident*.

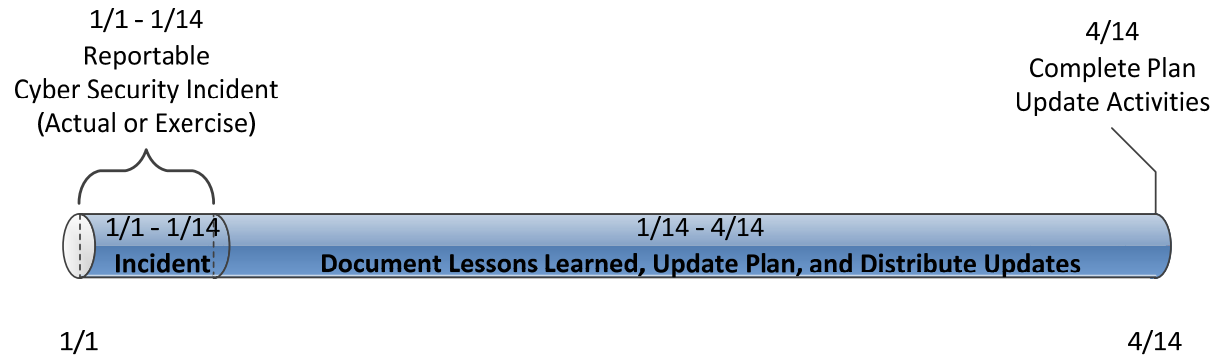


Figure 1: CIP-008-5 R3 Timeline for Reportable Cyber Security Incidents

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the incident and documenting the lessons learned as soon after the incident as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the incident response team.

The plan change requirement in Part 3.2 is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.

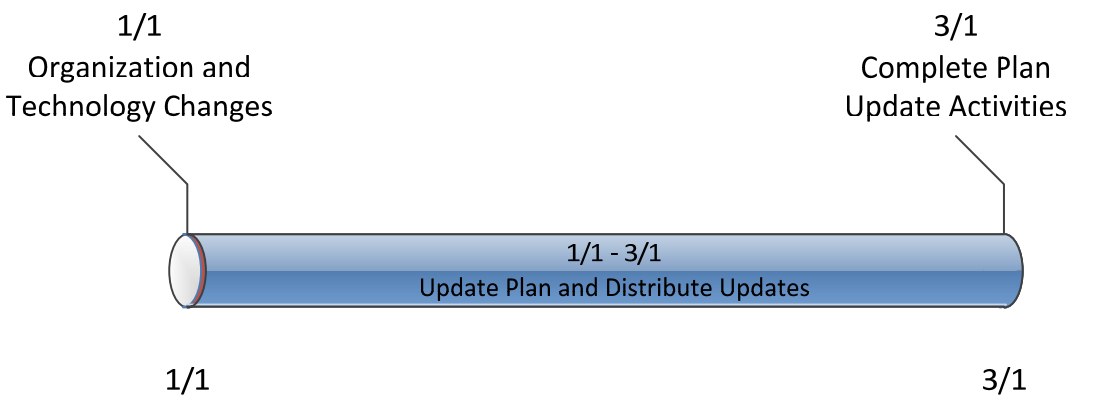


Figure 2: Timeline for Plan Changes in 3.2

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. An enterprise or single incident response plan for all BES Cyber Systems may be used to meet the Requirement. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: Wording changes have been incorporated based primarily on industry feedback to more specifically describe required actions.

Reference to prior version: (Part 1.1) CIP-008, R1.1

Change Description and Justification: (Part 1.1)

"Characterize" has been changed to "identify" for clarity. "Response actions" has been changed to "respond to" for clarity.

Reference to prior version: (Part 1.2) CIP-008, R1.1

Change Description and Justification: (Part 1.2)

Addresses the reporting requirements from previous versions of CIP-008. This requirement part only obligates entities to have a process for determining Reportable Cyber Security Incidents. Also addresses the directive in FERC Order No. 706, paragraphs 673 and 676 to report within one hour (at least preliminarily).

Reference to prior version: (Part 1.3) CIP-008, R1.2

Change Description and Justification: (Part 1.3)

Replaced incident response teams with incident response "groups or individuals" to avoid the interpretation that roles and responsibilities sections must reference specific teams.

Reference to prior version: (Part 1.4) CIP-008, R1.2

Change Description and Justification: (Part 1.4)
Conforming change to reference new defined term Cyber Security Incidents.

Rationale for R2:

The implementation of an effective Cyber Security Incident response plan mitigates the risk to the reliable operation of the BES caused as the result of a Cyber Security Incident and provides feedback to Responsible Entities for improving the security controls applying to BES Cyber Systems. This requirement ensures implementation of the response plans. Requirement Part 2.3 ensures the retention of incident documentation for post event analysis.

This requirement obligates entities to follow the Cyber Security Incident response plan when an incident occurs or when testing, but does not restrict entities from taking needed deviations from the plan. It ensures the plan represents the actual response and does not exist for documentation only. If a plan is written at a high enough level, then every action during the response should not be subject to scrutiny. The plan will likely allow for the appropriate variance in tactical decisions made by incident responders. Deviations from the plan can be documented during the incident response or afterward as part of the review.

Summary of Changes: Added testing requirements to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Reference to prior version: (Part 2.1) CIP-008, R1.6

Change Description and Justification: (Part 2.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-008, R1.6

Change Description and Justification: (Part 2.2)

Allows deviation from plan(s) during actual events or testing if deviations are recorded for review.

Reference to prior version: (Part 2.3) CIP-008, R2

Change Description and Justification: (Part 2.3)

Removed references to the retention period because the Standard addresses data retention in the Compliance Section.

Rationale for R3:

Conduct sufficient reviews, updates and communications to verify the Responsible Entity's response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System. A separate plan is not required for those requirement parts of the table applicable to High or Medium Impact BES Cyber Systems. If an entity has a single Cyber Security Incident response plan and High or Medium Impact BES Cyber Systems, then the additional requirements would apply to the single plan.

Summary of Changes: Changes here address the FERC Order 706, Paragraph 686, which includes a directive to perform after-action review for tests or actual incidents and update the plan based on lessons learned. Additional changes include specification of what it means to review the plan and specification of changes that would require an update to the plan.

Reference to prior version: (Part 3.1) CIP-008, R1.5

Change Description and Justification: (Part 3.1)

Addresses FERC Order 706, Paragraph 686 to document test or actual incidents and lessons learned.

Reference to prior version: (Part 3.2) CIP-008, R1.4

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	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.**~~Responsible Entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated ~~**Version**~~version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
~~4~~5	~~Board approved 01/24/2011~~11/ 26/12	~~**Update version number from "3" to "4"**~~Adopted by the NERC Board of Trustees.	~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.
~~**4**~~	~~4/19/12~~	~~FERC Order issued approving CIP-008-4 (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

A. Introduction

1. Title: Cyber Security — Recovery Plans for BES Cyber Systems

2. Number: CIP-009-5

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-009-5:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, CIP-009-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.
R2	**Operations**	**Lower**	The Responsible	The Responsible	The Responsible	The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Planning **Real-time Operations**		Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any	Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were	Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

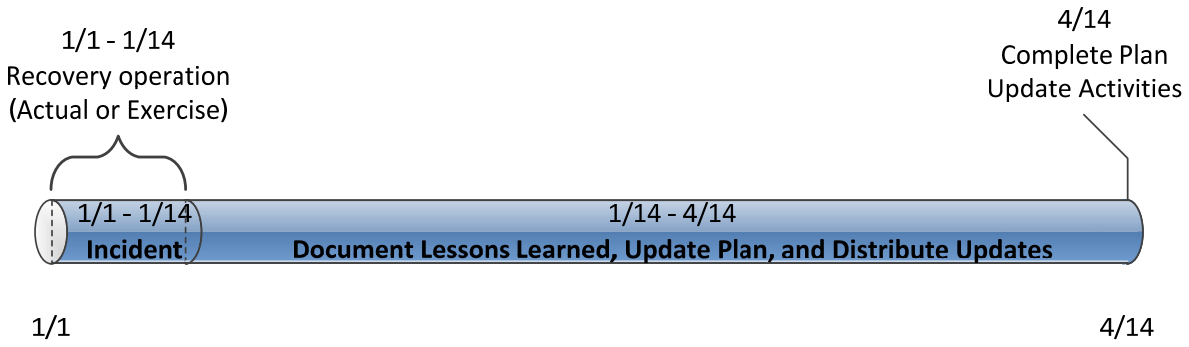


Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

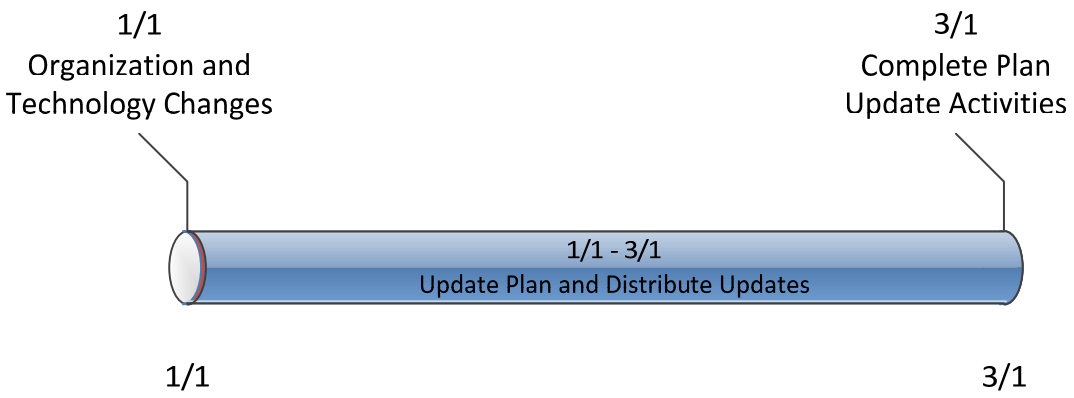


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	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. Changed compliance monitor to Compliance Enforcement Authority.	

3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.

A. Introduction

1. Title: Cyber Security — Recovery Plans for CriticalBES Cyber AssetsSystems

2. Number: CIP-009-45

3. Purpose: Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

3. Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

4. Applicability:

4.1. Within the text of Standard CIP-009-3, "Responsible Entity" shall mean:

4.1.1 Reliability Coordinator

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.24.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

~~4.1.3~~4.1.5 Interchange Coordinator or Interchange Authority

~~4.1.4 Transmission Service Provider~~

4.1.6 Reliability Coordinator

~~4.1.5~~4.1.7 Transmission ~~Owner~~Operator

~~4.1.6 Transmission Operator~~

~~4.1.7~~4.1.8 ~~Generator~~ Owner

~~4.1.8 Generator Operator~~

~~4.1.9 Load Serving Entity~~

~~4.1.10 NERC~~

~~4.1.11 Regional Entity~~

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first

interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

~~4.2.~~4.2.3 Exemptions: The following are exempt from Standard CIP-009-~~4:~~5:

~~4.2.1~~4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

~~4.2.2~~4.2.3.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

~~4.2.3~~4.2.3.3 ~~In nuclear plants, the~~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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

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

4.2.3.5 ~~**Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (~~Systems categorized as high impact or medium impact according to the ~~Reliability Standard otherwise becomes~~CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-009-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after ~~BOT adoption in~~the effective date of the order providing applicable regulatory approval.

~~5.~~ 2. In those jurisdictions where no regulatory approval is ~~not~~ required~~).~~

~~B. Requirements~~

~~R1.~~ ~~Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s), CIP-009-5~~ shall ~~address at a minimum the~~ become effective on the first day of the ninth calendar quarter following~~:~~

~~1.1.~~ ~~Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).~~

~~1.2.~~ ~~Define the roles and responsibilities of responders.~~

~~R2.~~ ~~Exercises — The recovery plan(s) shall be exercised at least annually. An exercise~~ Board of ~~the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.~~

R3. Change Control — Recovery plan(s) shall be updated to reflect any changesTrustees' approval, or lessons learned as a result of an exercise or as otherwise made effective pursuant to 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 completedlaws applicable to such ERO governmental authorities.

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.

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.

C. Measures

The 6. Background:

Standard CIP-009-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

M1. Each Responsible Entity shall make available its recovery plan(s) as specified in Requirement R1implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

M2. The Responsible Entity shall make available its records documenting required exercises as specified in Requirement R2.

M3. The Responsible Entity shall make available its documentation of changes to the recovery plan(s), and documentation of all communications, as specified in Requirement R3.

~~**M4.** The Responsible Entity shall make available its documentation regarding backup and storage of information as specified in Requirement R4.~~

~~**M5.** The Responsible Entity shall make available its documentation of testing of backup media as specified in Requirement R5.~~

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.

- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to BES Cyber Systems located at a Control Center and categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.

B. Requirements and Measures

R1. Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*. *[Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].*

M1. Evidence must include the documented recovery plan(s) that collectively include the applicable requirement parts in *CIP-009-5 Table R1 – Recovery Plan Specifications*.

CIP-009-5 Table R1 – Recovery Plan Specifications

Part	Applicable Systems	Requirements	Measures
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Conditions for activation of the recovery plan(s).	An example of evidence may include, but is not limited to, one or more plans that include language identifying conditions for activation of the recovery plan(s).
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Roles and responsibilities of responders.	An example of evidence may include, but is not limited to, one or more recovery plans that include language identifying the roles and responsibilities of responders.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	An example of evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information required to recover BES Cyber System functionality.

CIP-009-5 Table R1 – Recovery Plan Specifications			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
1.5	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, its documented recovery plan(s) to collectively include each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable requirement parts in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing.*

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	An example of evidence may include, but is not limited to, dated evidence of a test (by recovering from an actual incident, with a paper drill or tabletop exercise, or with an operational exercise) of the recovery plan at least once every 15 calendar months. For the paper drill or full operational exercise, evidence may include meeting notices, minutes, or other records of exercise findings.

CIP-009-5 Table R2 – Recovery Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	An example of evidence may include, but is not limited to, operational logs or test results with criteria for testing the usability (e.g. sample tape load, browsing tape contents) and compatibility with current system configurations (e.g. manual or automated comparison checkpoints between backup media contents and current configuration).
2.3	High Impact BES Cyber Systems	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Examples of evidence may include, but are not limited to, dated documentation of: • An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or • An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.

R3. Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].*

M3. Acceptable evidence includes, but is not limited to, each of the applicable requirement parts in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication.*

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 90 calendar days after completion of a recovery plan test or actual recovery: 3.1.1. Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned; 3.1.2. Update the recovery plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	An example of evidence may include, but is not limited to, all of the following: 1. Dated documentation of identified deficiencies or lessons learned for each recovery plan test or actual incident recovery or dated documentation stating there were no lessons learned; 2. Dated and revised recovery plan showing any changes based on the lessons learned; and 3. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems at Control Centers and their associated: 1. EACMS; and 2. PACS	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: 3.2.1. Update the recovery plan; and 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	An example of evidence may include, but is not limited to, all of the following: 1. Dated and revised recovery plan with changes to the roles or responsibilities, responders, or technology; and 2. Evidence of plan update distribution including, but not limited to: • Emails; • USPS or other mail service; • Electronic distribution system; or • Training sign-in sheets.

D.C. 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, theThe 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, ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authoritiesauthority shall serve as the Compliance Enforcement AuthorityCEA.

1.2. For the ERO, a third-party monitor without vested interest**Evidence Retention:**

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in the outcomethis standard for the EROthree calendar years.

1.2.4• If a Responsible Entity is found non-compliant, it shall serve askeep information related to the non-compliance until mitigation is complete and approved or for the Compliance Enforcement Authoritytime specified above, whichever is longer.

- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement**Assessment** Processes:

- Compliance AuditsAudit
- Self-CertificationsCertification
- Spot Checking
- Compliance Violation InvestigationsInvestigation
- Self-Reporting

Complaints

1.4. Data Retention

~~1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-009-4 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.~~

- Complaint

~~1.5.~~1.4. Additional Compliance Information~~:~~

~~2. Violation Severity Levels~~

- None

2. Table of Compliance Elements

~~R #~~ Requirement	Time Horizon	~~VRF~~ VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	~~MEDIUM~~Medium	N/A	The Responsible Entity has ~~not annually reviewed~~developed recovery plan(s~~) for Critical Cyber Assets.~~), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has ~~created~~developed recovery plan(s~~) for Critical Cyber Assets~~), but ~~did~~the plan(s) do not address ~~one~~two of the requirements ~~CIP-009-4 R1~~ included in Parts 1~~ or R1~~.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for ~~Critical~~BES Cyber ~~Assets that~~Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address ~~at a minimum both~~the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of

R # Requirement	Time Horizon	VRF VRF	Violation Severity Levels (CIP-009-5) Lower VSL	Moderate VSL	High VSL	Severe VSL
						the requirements CIP-009-4 R1.1 and R1in Parts 1.2 through 1.5.
R1.1.	MEDIUM	N/A	N/A	N/A	N/A	
R1.2.	MEDIUM	N/A	N/A	N/A	N/A	
R2	LOWER	N/A	N/A	N/A	The Responsible Entity's recovery plan(s) have not been exercised at least annually.	
R3R2	Operations Planning Real-time Operations	LOWERLower	The Responsible Entity'sEntity has not tested the recovery plan(s) have been updatedaccording to reflectR2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the	The Responsible Entity's recovery plan(s) have been updated to reflect any changes or lessons learned as a result of an exercise orEntity has not tested the recovery from an actual incident but the updatesplan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were communicated to personnel responsible for the activation	The Responsible Entity'sEntity has not tested the recovery plan(s) have been updatedaccording to reflectR2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any changes or lessons learned as a result of an exercise or the recovery from an actual incident but the	The Responsible Entity's recovery plan(s) haveEntity has not been updated to reflect any changes or lessons learned as a result of an exercise or tested the recovery from an actual incident.plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR

			updatesdeficiencies were communicated to personnel responsible for the activation and implementationidentified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan(s) in more than 30 but less than or equal	and implementationidentified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan(s) in more than 120 but less than or equal to 150 calendar days of the change. according to R2 Part 2.3 within 37	updatesdeficiencies were communicated to personnel responsible for the activation and implementationidentified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan(s) in more than 150	The Responsible Entity's Entity has tested the recovery plan(s) have been updatedaccording to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incidentR2 Part 2.1 and identified deficiencies, but the updates were communicated to personnel responsible fordid not assess or correct the activation and implementation of deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in more than 180 calendar

			according to 120 calendar days of the change.R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	but less than or equal according to 180 calendar days of the change.R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	daysthe recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the change.information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System

						functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

						Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R4R3	**Operations Assessment**	LOWERLower	N/AThe Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	N/AThe Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the	N/AThe Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR	The Responsible Entity's Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan(s) do not include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. test or actual recovery. (3.1.1)

				recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	

R5		LOWER	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.

~~E.~~D. Regional Variances

None ~~identified~~.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

The following guidelines are available to assist in addressing the required components of a recovery plan:

- NERC, Security Guideline for the Electricity Sector: Continuity of Business Processes and Operations Operational Functions, September 2011, online at http://www.nerc.com/docs/cip/sgwg/Continuity%20of%20Business%20and%20Operational%20Functions%20FINAL%20102511.pdf
- National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 revision 1, May 2010, online at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

The term recovery plan is used throughout this Standard to refer to a documented set of instructions and resources needed to recover reliability functions performed by BES Cyber Systems. The recovery plan may exist as part of a larger business continuity or disaster recovery plan, but the term does not imply any additional obligations associated with those disciplines outside of the Requirements.

A documented recovery plan may not be necessary for each applicable BES Cyber System. For example, the short-term recovery plan for a BES Cyber System in a specific substation may be

managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for BES Cyber Systems should suffice for several similar facilities such as those found in substations or power plants' facilities.

For Part 1.1, the conditions for activation of the recovery plan should consider viable threats to the BES Cyber System such as natural disasters, computing equipment failures, computing environment failures, and Cyber Security Incidents. A business impact analysis for the BES Cyber System may be useful in determining these conditions.

For Part 1.2, entities should identify the individuals required for responding to a recovery operation of the applicable BES Cyber System.

For Part 1.3, entities should consider the following types of information to recover BES Cyber System functionality:

1. Installation files and media;
2. Current backup tapes and any additional documented configuration settings;
3. Documented build or restoration procedures; and
4. Cross site replication storage.

For Part 1.4, the processes to verify the successful completion of backup processes should include checking for: (1) usability of backup media, (2) logs or inspection showing that information from current, production system could be read, and (3) logs or inspection showing that information was written to the backup media. Test restorations are not required for this Requirement Part. The following backup scenarios provide examples of effective processes to verify successful completion and detect any backup failures:

- Periodic (e.g. daily or weekly) backup process – Review generated logs or job status reports and set up notifications for backup failures.
- Non-periodic backup process– If a single backup is provided during the commissioning of the system, then only the initial and periodic (every 15 months) testing must be done. Additional testing should be done as necessary and can be a part of the configuration change management program.
- Data mirroring – Configure alerts on the failure of data transfer for an amount of time specified by the entity (e.g. 15 minutes) in which the information on the mirrored disk may no longer be useful for recovery.
- Manual configuration information – Inspect the information used for recovery prior to storing initially and periodically (every 15 months). Additional inspection should be done as necessary and can be a part of the configuration change management program.

The plan must also include processes to address backup failures. These processes should specify the response to failure notifications or other forms of identification.

For Part 1.5, the recovery plan must include considerations for preservation of data to determine the cause of a Cyber Security Incident. Because it is not always possible to initially

know if a Cyber Security Incident caused the recovery activation, the data preservation procedures should be followed until such point a Cyber Security Incident can be ruled out. CIP-008 addresses the retention of data associated with a Cyber Security Incident.

Requirement R2:

A Responsible Entity must exercise each BES Cyber System recovery plan every 15 months. However, this does not necessarily mean that the entity must test each plan individually. BES Cyber Systems that are numerous and distributed, such as those found at substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers differ a great deal from those associated with power plants and substations.

A recovery plan test does not necessarily cover all aspects of a recovery plan and failure scenarios, but the test should be sufficient to ensure the plan is up to date and at least one restoration process of the applicable cyber systems is covered.

Entities may use an actual recovery as a substitute for exercising the plan every 15 months. Otherwise, entities must exercise the plan with a paper drill, tabletop exercise, or operational exercise. For more specific types of exercises, refer to the FEMA Homeland Security Exercise and Evaluation Program (HSEEP). It lists the following four types of discussion-based exercises: seminar, workshop, tabletop, and games. In particular, it defines that, "A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. [Table top exercises (TTX)] can be used to assess plans, policies, and procedures."

The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, "[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims)."

For Part 2.2, entities should refer to the backup and storage of information required to recover BES Cyber System functionality in Requirement Part 1.3. This provides additional assurance that the information will actually recover the BES Cyber System as necessary. For most complex computing equipment, a full test of the information is not feasible. Entities should determine the representative sample of information that provides assurance in the processes for Requirement Part 1.3. The test must include steps for ensuring the information is useable and current. For backup media, this can include testing a representative sample to make sure the information can be loaded, and checking the content to make sure the information reflects the current configuration of the applicable Cyber Assets.

Requirement R3:

This requirement ensures entities maintain recovery plans. There are two requirement parts that trigger plan updates: (1) lessons learned and (2) organizational or technology changes.

The documentation of lessons learned is associated with each recovery activation, and it involves the activities as illustrated in Figure 1, below. The deadline to document lessons learned starts after the completion of the recovery operation in recognition that complex recovery activities can take a few days or weeks to complete. The process of conducting lessons learned can involve the recovery team discussing the incident to determine gaps or areas of improvement within the plan. It is possible to have a recovery activation without any documented lessons learned. In such cases, the entity must retain documentation of the absence of any lessons learned associated with the recovery activation.

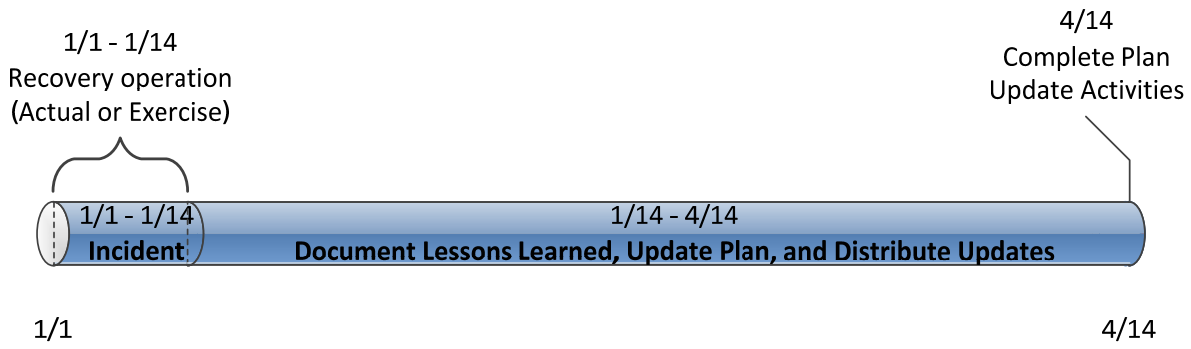


Figure 1: CIP-009-5 R3 Timeline

The activities necessary to complete the lessons learned include updating the plan and distributing those updates. Entities should consider meeting with all of the individuals involved in the recovery and documenting the lessons learned as soon after the recovery activation as possible. This allows more time for making effective updates to the plan, obtaining any necessary approvals, and distributing those updates to the recovery team.

The plan change requirement is associated with organization and technology changes referenced in the plan and involves the activities illustrated in Figure 2, below. Organizational changes include changes to the roles and responsibilities people have in the plan or changes to the response groups or individuals. This may include changes to the names or contact information listed in the plan. Technology changes affecting the plan may include referenced information sources, communication systems, or ticketing systems.

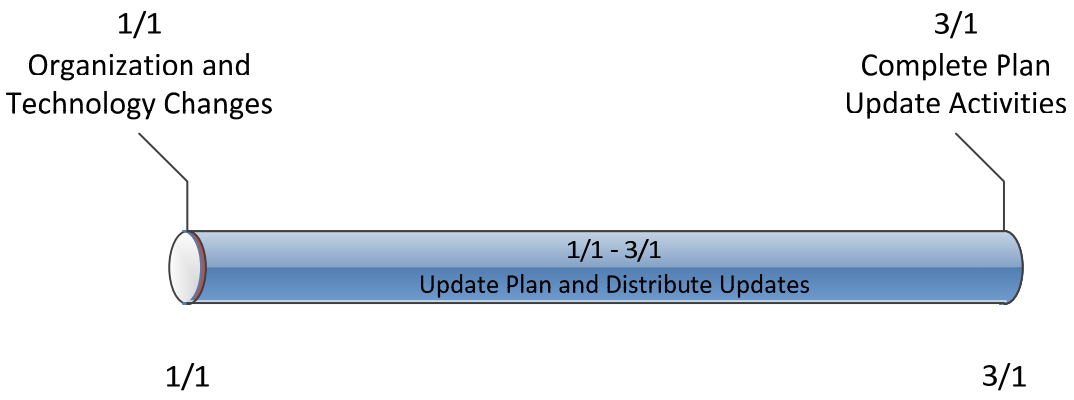


Figure 2: Timeline for Plan Changes in 3.2

When notifying individuals of response plan changes, entities should keep in mind that recovery plans may be considered BES Cyber System Information, and they should take the appropriate measures to prevent unauthorized disclosure of recovery plan information. For example, the recovery plan itself, or other sensitive information about the recovery plan, should be redacted from Email or other unencrypted transmission.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

Summary of Changes: Added provisions to protect data that would be useful in the investigation of an event that results in the need for a Cyber System recovery plan to be utilized.

Reference to prior version: (Part 1.1) CIP-009, R1.1

Change Description and Justification: (Part 1.1)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.2) CIP-009, R1.2

Change Description and Justification: (Part 1.2)

Minor wording changes; essentially unchanged.

Reference to prior version: (Part 1.3) CIP-009, R4

Change Description and Justification: (Part 1.3)

Addresses FERC Order Paragraph 739 and 748. The modified wording was abstracted from Paragraph 744.

Reference to prior version: (Part 1.4) New Requirement

Change Description and Justification: (Part 1.4)

Addresses FERC Order Section 739 and 748.

Reference to prior version: (Part 1.5) New Requirement

Change Description and Justification: (Part 1.5)

Added requirement to address FERC Order No. 706, Paragraph 706.

Rationale for R2:

The implementation of an effective recovery plan mitigates the risk to the reliable operation of the BES by reducing the time to recover from various hazards affecting BES Cyber Systems. This requirement ensures continued implementation of the response plans.

Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information.

Summary of Changes. Added operational testing for recovery of BES Cyber Systems.

Reference to prior version: (Part 2.1) CIP-009, R2

Change Description and Justification: (Part 2.1)

Minor wording change; essentially unchanged.

Reference to prior version: (Part 2.2) CIP-009, R5

Change Description and Justification: (Part 2.2)

Specifies what to test and makes clear the test can be a representative sampling. These changes, along with Requirement Part 1.4 address the FERC Order No. 706, Paragraphs 739 and 748 related to testing of backups by providing high confidence the information will actually recover the system as necessary.

Reference to prior version: (Part 2.3) CIP-009, R2

Change Description and Justification: (Part 2.3)

Addresses FERC Order No. 706, Paragraph 725 to add the requirement that the recovery plan test be a full operational test once every 3 years.

Rationale for R3:

To improve the effectiveness of BES Cyber System recovery plan(s) following a test, and to ensure the maintenance and distribution of the recovery plan(s). Responsible Entities achieve this by (i) performing a lessons learned review in 3.1 and (ii) revising the plan in 3.2 based on specific changes in the organization or technology that would impact plan execution. In both instances when the plan needs to change, the Responsible Entity updates and distributes the plan.

Summary of Changes: Makes clear when to perform lessons learned review of the plan and specifies the timeframe for updating the recovery plan.

Reference to prior version: (Part 3.1) CIP-009, R1 and R3

Change Description and Justification: (Part 3.1)

Added the timeframes for performing lessons learned and completing the plan updates. This requirement combines all three activities in one place. Where previous versions specified 30 calendar days for performing lessons learned, followed by additional time for updating recovery plans and notification, this requirement combines those activities into a single timeframe.

Reference to prior version: (Part 3.2) New Requirement

Change Description and Justification: (Part 3.2)

Specifies the activities required to maintain the plan. The previous version required entities to update the plan in response to any changes. The modifications make clear the specific changes that would require an update.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	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.**~~Responsible Entity. Rewording of Effective Date. ~~Communication of revisions to the recovery~~	

		~~plan changed from 90 days to 30 days.~~ Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version ~~**numbers**~~number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees.	Update
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	
~~4~~5	~~Board approved 01/24/2011~~1/26/12	~~**Update version number from "3" to "4"**~~Adopted by the NERC Board of Trustees.	~~Update to conform to changes to CIP-002-4 (Project 2008-06)~~Modified to coordinate with other CIP standards and to revise format to use RBS Template.
~~**4**~~	~~4/19/12~~	~~FERC Order issued approving CIP-009-4 (approval becomes effective June 25, 2012)~~ ~~Added approved VRF/VSL table to section D.2.~~	

A. Introduction

1. Title: Cyber Security — Configuration Change Management and Vulnerability Assessments

2. Number: CIP-010-1

3. Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-010-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-010-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-010-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-010-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented processes, but they must address the applicable requirements in the table. The

documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:

Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management Framework as a way of applying requirements more appropriately

based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)**– Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)**– Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-1 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

R2. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-1 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment,; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-1 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for	implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline	changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update	the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies in the verification documentation. (1.4.3)	configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the	The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in	required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies.	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					(1.5.1) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems.	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(3.2)			its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be

included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-5. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-5 R2.1 requires entities to track, evaluate, and install security patches, CIP-010 R1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.

3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Reference to prior version: (Part 1.1) New Requirement

Change Rationale: (Part 1.1)

The baseline configuration requirement was incorporated from the DHS Catalog for Control Systems Security. The baseline requirement is also intended to clarify precisely when a change management process must be invoked and which elements of the configuration must be examined.

Reference to prior version: (Part 1.2) CIP-007-3, R9; CIP-003-3, R6

Change Rationale: (Part 1.2)

The SDT added requirement to explicitly authorize changes. This requirement was previously implied by CIP-003-3, Requirement R6.

Reference to prior version: (Part 1.3) CIP-007-3, R9; CIP-005-3, R5

Change Rationale: (Part 1.3)

Document maintenance requirement due to a BES Cyber System change is equivalent to the requirements in the previous versions of the standard.

Reference to prior version: (Part 1.4) CIP-007-3, R1

Change Rationale: (Part 1.4)

The SDT attempted to provide clarity on when testing must occur and removed requirement for specific test procedures because it is implicit in the performance of the requirement.

Reference to prior version: (Part 1.5) CIP-007-3, R1

Change Rationale: (Part 1.5)

This requirement provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed.

This change addresses FERC Order No. 706, Paragraphs 397, 609, 610, and 611.

Rationale for R2:

The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Reference to prior version: (Part 2.1) New Requirement

Change Rationale: (Part 2.1)

The monitoring of the configuration of the BES Cyber System provides an express acknowledgement of the need to consider malicious actions along with intentional changes.

This requirement was added after review of the DHS Catalog of Control System Security and to address FERC Order No. 706, Paragraph 397.
Thirty-five Calendar days allows for a "once-a-month" frequency with slight flexibility to account for months with 31 days or for beginning or endings of months on weekends.

Rationale for R3:

The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.

The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Reference to prior version: (Part 3.1) CIP-005-4, R4; CIP-007-4, R8

Change Rationale: (Part 3.1)

As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.

Reference to prior version: (Part 3.2) New Requirement

Change Rationale: (Part 3.2)

FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.

As suggested in FERC Order No. 706, Paragraph 644, the details for what should be included in the assessment are left to guidance.

Reference to prior version: (Part 3.3) New Requirement

Change Rationale: (Part 3.3)
FERC Order No. 706, Paragraphs 541, 542, 543, 544, 545, and 547.

Reference to prior version: (Part 3.4) CIP-005-3, R4.5; CIP-007-3, R8.4

Change Rationale: (Part 3.4)
Added a requirement for an entity planned date of completion as per the directive in FERC Order No. 706, Paragraph 643.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.

A. Introduction

1. Title: Cyber Security — Information Protection

2. Number: CIP-011-1

3. Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

4.1.2.1 Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

4.1.2.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.1.2.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.1.2.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.1.2.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each Special Protection System or Remedial Action Scheme where the Special Protection System or Remedial Action Scheme is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers:

All BES Facilities.

4.2.3 Exemptions: The following are exempt from Standard CIP-011-1:

4.2.3.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

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

4.2.3.3 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.

4.2.3.4 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes.

5. Effective Dates:

1. **24 Months Minimum** – CIP-011-1 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.

2. In those jurisdictions where no regulatory approval is required, CIP-011-1 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

Standard CIP-011-1 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Most requirements open with, "*Each Responsible Entity shall implement one or more documented [processes, plan, etc] that include the applicable items in [Table Reference].*" The referenced table requires the applicable items in the procedures for the requirement's common subject matter.

The SDT has incorporated within this standard a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. It is presented in those requirements by modifying "implement" as follows:

> Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** . . .

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements. An entity should include as much as it believes necessary in their documented

processes, but they must address the applicable requirements in the table. The documented processes themselves are not required to include the ". . . identifies, assesses, and corrects deficiencies, . . ." elements described in the preceding paragraph, as those aspects are related to the manner of implementation of the documented processes and could be accomplished through other controls or compliance management activities.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e., incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.
Responsible Entities can implement common controls that meet requirements for multiple high and medium impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

Throughout the standards, unless otherwise stated, bulleted items in the requirements and measures are items that are linked with an "or," and numbered items are items that are linked with an "and."

Many references in the Applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

"Applicable Systems" Columns in Tables:
Each table has an "Applicable Systems" column to further define the scope of systems to which a specific requirement row applies. The CSO706 SDT adapted this concept from the National Institute of Standards and Technology ("NIST") Risk Management

Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the "Applicable Systems" column as described.

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)**– Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System

B. Requirements and Measures

R1. Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence for the information protection program must include the applicable requirement parts in *CIP-011-1 Table R1 – Information Protection* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Method(s) to identify information that meets the definition of BES Cyber System Information.	Examples of acceptable evidence include, but are not limited to: • Documented method to identify BES Cyber System Information from entity's information protection program; or • Indications on information (e.g., labels or classification) that identify BES Cyber System Information as designated in the entity's information protection program; or • Training materials that provide personnel with sufficient knowledge to recognize BES Cyber System Information; or • Repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program.

CIP-011-1 Table R1 – Information Protection			
Part	**Applicable Systems**	**Requirement**	**Measure**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS Medium Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PACS	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Examples of acceptable evidence include, but are not limited to: • Procedures for protecting and securely handling, which include topics such as storage, security during transit, and use of BES Cyber System Information; or • Records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented procedure(s).

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

- Compliance Audit
- Self-Certification
- Spot Checking
- Compliance Investigation
- Self-Reporting
- Complaint

1.4. Additional Compliance Information:

- None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify,	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 – Scope of Applicability of the CIP Cyber Security Standards

Section "4. Applicability" of the standards provides important information for Responsible Entities to determine the scope of the applicability of the CIP Cyber Security Requirements.

Section "4.1. Functional Entities" is a list of NERC functional entities to which the standard applies. If the entity is registered as one or more of the functional entities listed in Section 4.1, then the NERC CIP Cyber Security Standards apply. Note that there is a qualification in Section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2. Furthermore,

Section "4.2. Facilities" defines the scope of the Facilities, systems, and equipment owned by the Responsible Entity, as qualified in Section 4.1, that is subject to the requirements of the standard. As specified in the exemption section 4.2.3.5, this standard does not apply to Responsible Entities that do not have High Impact or Medium Impact BES Cyber Systems under CIP-002-5's categorization. In addition to the set of BES Facilities, Control Centers, and other systems and equipment, the list includes the set of systems and equipment owned by Distribution Providers. While the NERC Glossary term "Facilities" already includes the BES characteristic, the additional use of the term BES here is meant to reinforce the scope of applicability of these Facilities where it is used, especially in this applicability scoping section. This in effect sets the scope of Facilities, systems, and equipment that is subject to the standards.

Requirement R1:

Responsible Entities are free to utilize existing change management and asset management systems. However, the information contained within those systems must be evaluated, as the information protection requirements still apply.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

This requirement mandates that BES Cyber System Information be identified. The Responsible Entity has flexibility in determining how to implement the requirement. The Responsible Entity should explain the method for identifying the BES Cyber System Information in their information protection program. For example, the Responsible Entity may decide to mark or label the documents. Identifying separate classifications of BES Cyber System Information is not specifically required. However, a Responsible Entity maintains the flexibility to do so if they desire. As long as the Responsible Entity's information protection program includes all applicable items, additional classification levels (e.g., confidential, public, internal use only, etc.) can be created that go above and beyond the requirements. If the entity chooses to use classifications, then the types of classifications used by the entity and any associated labeling should be documented in the entity's BES Cyber System Information Program.

The Responsible Entity may store all of the information about BES Cyber Systems in a separate repository or location (physical and/or electronic) with access control implemented. For example, the Responsible Entity's program could document that all information stored in an identified repository is considered BES Cyber System Information, the program may state that all information contained in an identified section of a specific repository is considered BES Cyber System Information, or the program may document that all hard copies of information are stored in a secured area of the building. Additional methods for implementing the requirement are suggested in the measures section. However, the methods listed in measures are not meant to be an exhaustive list of methods that the entity may choose to utilize for the identification of BES Cyber System Information.

The SDT does not intend that this requirement cover publicly available information, such as vendor manuals that are available via public websites or information that is deemed to be publicly releasable.

Information protection pertains to both digital and hardcopy information. R1.2 requires one or more procedures for the protection and secure handling BES Cyber System Information, including storage, transit, and use.

The entity's written Information Protection Program should explain how the entity handles aspects of information protection including specifying how BES Cyber System Information is to be securely handled during transit in order to protect against unauthorized access, misuse, or corruption and to protect confidentiality of the communicated BES Cyber System Information. For example, the use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption to prevent unauthorized disclosure of information during transmission. The entity may choose to establish a trusted communications path for transit of BES Cyber System Information. The trusted communications path would utilize a logon or other security measures to provide secure handling during transit. The entity may employ alternative physical protective measures, such as the use of a courier or locked container for transmission of information. It is not the intent of this standard to mandate the use of one particular format for secure handling during transit.

A good Information Protection Program will document the circumstances under which BES Cyber System Information can be shared with or used by third parties. The organization should distribute or share information on a need-to-know basis. For example, the entity may specify that a confidentiality agreement, non-disclosure arrangement, contract, or written agreement of some kind concerning the handling of information must be in place between the entity and the third party. The entity's Information Protection Program should specify circumstances for sharing of BES Cyber System Information with and use by third parties, for example, use of a non-disclosure agreement. The entity should then follow their documented program. These requirements do not mandate one specific type of arrangement.

Requirement R2:

This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact, as that should not constitute a release for reuse. However, following the

analysis, if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media.

The justification for this requirement is pre-existing from previous versions of CIP and is also documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking.

If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2.

Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed. Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances, such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.

The following information from NIST SP800-88 provides additional guidance concerning the types of actions that an entity might take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media:

> Clear: One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
>
> Purge: Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36] Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging.

Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Destroy: There are many different types, techniques, and procedures for media destruction. Disintegration, Pulverization, Melting, and Incineration are sanitization methods designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning.

In some cases such as networking equipment, it may be necessary to contact the manufacturer for proper sanitization procedure.

It is critical that an organization maintain a record of its sanitization actions to prevent unauthorized retrieval of BES Cyber System Information. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes.

Rationale:

During the development of this standard, references to prior versions of the CIP standards and rationale for the requirements and their parts were embedded within the standard. Upon BOT approval, that information was moved to this section.

Rationale for R1:

The SDT's intent of the information protection program is to prevent unauthorized access to BES Cyber System Information.

Summary of Changes: CIP 003-4 R4, R4.2, and R 4.3 have been moved to CIP 011 R1. CIP-003-4, Requirement R4.1 was moved to the definition of BES Cyber System Information.

Reference to prior version: (Part 1.1) CIP-003-3, R4; CIP-003-3, R4.2

Change Rationale: (Part 1.1)

The SDT removed the explicit requirement for classification as there was no requirement to have multiple levels of protection (e.g., confidential, public, internal use only, etc.) This modification does not prevent having multiple levels of classification, allowing more flexibility for entities to incorporate the CIP information protection program into their normal business.

Reference to prior version: (Part 1.2) CIP-003-3, R4

Change Rationale: (Part 1.2)

The SDT changed the language from "protect" information to "Procedures for protecting and securely handling" to clarify the protection that is required.

Rationale for R2:

The intent of the BES Cyber Asset reuse and disposal process is to prevent the unauthorized dissemination of BES Cyber System Information upon reuse or disposal.

Reference to prior version: (Part 2.1) CIP-007-3, R7.2

Change Rationale: (Part 2.1)

Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.

Reference to prior version: (Part 2.2) CIP-007-3, R7.1

Change Rationale: (Part 2.2)

Consistent with FERC Order No. 706, Paragraph 631, the SDT clarified that the goal was to prevent the unauthorized retrieval of information from the media, removing the word "erase" since, depending on the media itself, erasure may not be sufficient to meet this goal.

The SDT also removed the requirement explicitly requiring records of destruction/redeployment as this was seen as demonstration of the existing requirement and not a requirement in and of itself.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the information protection requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.

Exhibit A

2.) Associated Modifications to the Glossary of Terms used in NERC Reliability Standards

Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

Electronic Access Control or Monitoring Systems ("EACMS")

Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.

Electronic Access Point ("EAP")

A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Intermediate System

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

Physical Access Control Systems ("PACS")

Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Protected Cyber Assets ("PCA")

One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is connected either to a Cyber Asset within the ESP or to the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Reportable Cyber Security Incident

A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets

Exhibit B

Implementation Plan for Proposed CIP Version 5 Reliability Standards
submitted for Approval

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Version 5 CIP Cyber Security Standards

October 26, 2012

Prerequisite Approvals

All Version 5 CIP Cyber Security Standards and the proposed additions, modifications, and retirements of terms to the *Glossary of Terms u*sed in *NERC Reliability Standards* must be approved before these standards can become effective.

Applicable Standards

The following standards and definitions, collectively referred to as "Version 5 CIP Cyber Security Standards,"[1] are covered by this Implementation Plan:

CIP–002–5 — Cyber Security — BES Cyber System Categorization
CIP–003–5 — Cyber Security — Security Management Controls
CIP–004–5 — Cyber Security — Personnel and Training
CIP–005–5 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–5 — Cyber Security — Physical Security of BES Cyber Systems
CIP–007–5 — Cyber Security — Systems Security Management
CIP–008–5 — Cyber Security — Incident Reporting and Response Planning
CIP–009–5 — Cyber Security — Recovery Plans for BES Cyber Systems
CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP–011–1 — Cyber Security — Information Protection

"Definitions of Terms used in Version 5 CIP Cyber Security Standards" document, which includes proposed additions, modifications, and retirements of terms to the *Glossary of Terms used in NERC Reliability Standards*.

These standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards are posted for ballot by NERC concurrently with this Implementation Plan.

When these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, all prior versions of these standards are retired.

[1] Although CIP-010-1 and CIP-011-1 are proposed as first versions, any reference to "Version 5 CIP Cyber Security Standards" includes CIP-010-1 and CIP-011-1, in addition to CIP-002-5 through CIP-009-5, because CIP-010-1 and CIP-011-1 were developed as part of the "Version 5 CIP Cyber Security Standards" development process.

Compliance with Standards

Once these standards and Definitions of Terms used in Version 5 CIP Cyber Security Standards become effective, the responsible entities identified in the Applicability Section of the standard must comply with the requirements.

Proposed Effective Date for Version 5 CIP Cyber Security Standards

Responsible entities shall comply with all requirements in CIP-002-5, CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1, and CIP-011-1 as follows:

1. **24 Months Minimum** – The Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval. CIP-003-5, Requirement R2, shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[2]
2. In those jurisdictions where no regulatory approval is required, the Version 5 CIP Cyber Security Standards, except for CIP-003-5 R2, shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, and CIP-003-5 R2 shall become effective on the first day of the 13th calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Initial Performance of Certain Periodic Requirements

Specific Version 5 CIP Cyber Security Standards have periodic requirements that contain time parameters for subsequent and recurring iterations of the requirement, such as, but not limited to, ". . . at least once every 15 calendar months . . .", and responsible entities shall comply initially with those periodic requirements as follows:

1. On or before the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-002-5, Requirement R2
   - CIP-003-5, Requirement R1
2. On or before the Effective Date of CIP-003-5, Requirement R2 for the following requirement:
   - CIP-003-5, Requirement R2

[2] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

3. Within 14 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-007-5, Requirement R4, Part 4.4
4. Within 35 calendar days after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-010-1, Requirement R2, Part 2.1
5. Within three calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R4, Part 4.2
6. Within 12 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-004-5, Requirement R2, Part 2.3
   - CIP-004-5, Requirement R4, Parts 4.3 and 4.4
   - CIP-006-5, Requirement R3, Part 3.1
   - CIP-008-5, Requirement R2, Part 2.1
   - CIP-009-5, Requirement R2, Parts 2.1, 2.2
   - CIP-010-1, Requirement R3, Parts 3.1
7. Within 24 calendar months after the Effective Date of the Version 5 CIP Cyber Security Standards for the following requirements:
   - CIP-009-5, Requirement R2, Part 2.3
   - CIP-010-1, Requirement R3, Part 3.2
8. Within 7 years after the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards for a personnel risk assessment for the following requirement:
   - CIP-004-5, Requirement R3, Part 3.5.

Previous Identity Verification

A documented identity verification performed pursuant to a previous version of the CIP Cyber Security Standards does not need to be reperformed under CIP-004-5, Requirement R3, Part 3.1.

Planned or Unplanned Changes Resulting in a Higher Categorization

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5, Requirement R2, which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change, and must, therefore, be in compliance with the Version 5 CIP Cyber Security Standards upon the commissioning of the modernized transmission substation.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to the following timelines, following the identification and categorization of the affected BES Cyber System and any applicable and associated Physical Access Control Systems, Electronic Access Control and Monitoring Systems and Protected Cyber Assets, with additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 months
New medium impact BES Cyber System	12 months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
Newly categorized medium impact BES Cyber System	12 months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 months

Applicability Reference Tables

The following tables are provided as a convenient reference to show which requirements in the Version 5 CIP Cyber Security Standards apply to specific Cyber Assets.

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-004-5 R2	Cyber Security Training Program	X	X	
CIP-004-5 R3	Personnel Risk Assessment Program	X	X	
CIP-004-5 R4	Access Management Program	X	X	
CIP-004-5 R5	Access Revocation	X	X	
CIP-005-5 R1 Part 1.2	Electronic Security Perimeter			X
CIP-005-5 R2	Remote Access Management			X
CIP-006-5 R1	Physical Security Plan	X	X	X
CIP-006-5 R2	Visitor Control Program	X		X
CIP-006-5 R3	Maintenance and Testing Program		X	

		Associated Electronic Access Control or Monitoring Systems	Physical Access Control System	Protected Cyber Assets
CIP-007-5 R1	Ports and Services	X	X	X
CIP-007-5 R2	Security Patch Management	X	X	X
CIP-007-5 R3	Malicious Code Prevention	X	X	X
CIP-007-5 R4	Security Event Monitoring	X	X	X
CIP-007-5 R5	System Access Control	X	X	X
CIP-010-1 R1	Configuration Change Management	X	X	X
CIP-010-1 R2	Configuration Monitoring	X	X	X
CIP-010-1 R3	Vulnerability Assessments	X	X	X
CIP-011-1 R1	Information Protection	X	X	
CIP-011-1 R2	BES Cyber Asset Reuse and Disposal	X	X	X

Exhibit C

Standard Drafting Team Roster for Project 2008-06 - Cyber Security Order 706 Version 5 CIP Standards

Project 2008-06 Standard Drafting Team Roster

Name and Title	Company and Address	Contact Info	Bio
Rob Antonishen, P. Eng. Section Manager, Controls and Metering Engineering and Technical Services	Ontario Power Generation 14000 Niagara Pkwy. Niagara-on-the-Lake, Ontario, Canada L0S 1J0	(905)262-2674 rob.antonishen@opg.com	After obtaining his BSc. in Electrical Engineering from Queens University in Kingston, Ontario, Canada, Rob began his 22 year career with Ontario Power Generation (then Ontario Hydro). Starting as field P&C Engineer, he has performed relaying, controls, governor, exciter and telecom maintenance, and led projects to replace hardwired relay controls with PLCs at hydro stations. He lead the teams designing, commissioning and administering OPG's corporate data acquisition and historian system, ICCP interfaces, and electronic dispatch systems. After a 5-year diversion though corporate IT and networking he is currently in Hydro-Thermal Operations as the corporate technical lead for CIP compliance, process control and cyber-security. Rob is also an active member of the NPCC Task Force on Infrastructure Security & Technology.
René Bourassa Engineer, Business Orientations, Systems & Security – Contrôle des mouvements d'énergie	Hydro-Québec TransÉnergie 6100 Des Forges, Trois-Rivières QC Canada G8Y 6K5	(819) 694-2507 bourassa.rene@hydro.qc.ca	René Bourassa is an engineer at Hydro-Québec and acts as a SCADA and Operational Technologies Cyber Security Expert. Mr. Bourassa began his 35 year career, of which more than 80% was spent in a Control Center environment, at Hydro-Québec on Gentilly nuclear power plants and Shawinigan 2 (the oldest hydraulic generation station still in operation in North America) operational activities while he was completing his Computer Science and Electrical Engineering Bachelor of Science degree. For 8 years, he taught "Programming for Engineers" and "Scientific Application Programming" at Université du Québec à Trois-Rivières. Besides his generation, transmission, and electric grid operation experience as an

Project 2008-06 Standard Drafting Team Roster

			electrical engineer, he also cumulated knowledge and experience in programming, system development, database, computer networks, computer and acquisition protocols, firewall, and other cyber security topics. Mr. Bourassa participated in commissioning one of Hydro-Québec's first Regional Telecontrol Center. As Telecontrol Main Architect and Cyber Security Coordinator, he was a major contributor to the evolution over the years of Hydro-Québec's telecontrol SCADA architecture, and he conceived and implemented the High Security Telecontrol Architecture. Since the late 1980s, he has promoted cyber security for SCADA systems and operational technology at Hydro-Québec and through presentations at RSA Conferences, SANS Process Control and SCADA Security Summits, EPRI GRPM/EIS PLC meetings, and participation in the DHS 2005 Roadmap to Secure Control Systems in the Energy Sector.
Jay Cribb Principal Information Security Analyst	Southern Company Services, Inc. 241 Ralph McGill Blvd NE Atlanta, GA 30308	(404)506-3854 jscribb@southernco.com	Jay Cribb has 27 years of experience in Information Technology within the electric utility industry. Jay is currently a Principal Information Security Analyst with Southern Company Services, Inc. where his responsibilities include working with Generation, Transmission, and numerous other business units in protecting critical infrastructure from cyber-based threats. He has been involved with the NERC CIP standards in some way since they were known as the '1200' standards. Jay has served in the past as the first cyber security representative for the SERC Region to the NERC CIPC. He has recently completed 2 years as vice-chair and 2 years as Chair of the EEI Security Committee. Jay was also the first chair of SERC's CIP Compliance working group and remains a member of the SERC CIPC.

Project 2008-06 Standard Drafting Team Roster

Sharon Edwards	Duke Energy		Sharon Edwards has worked for Duke Energy since 1989. She has served in a variety of roles and has been involved with implementing cyber security standards at Duke since the inception of Urgent Action 1200 for Cyber Security. At Duke Energy, Sharon is the Legacy Duke Program Lead for Critical Infrastructure Protection (CIP). She previously worked implementing cyber security and the associated regulations in the Telecom area at Duke. Sharon has been a member of the FERC Order 706 Standards Drafting Team since the beginning of the drafting team. She is also a member of the Critical Infrastructure Protection Committee. Ms. Edwards is a Certified Information Systems Security Professional (CISSP). She holds a bachelors degree from Xavier University in Cincinnati, Ohio, and a Master of Business Administration degree (MBA) from Thomas More College in northern Kentucky.
Gerald Freese Director, NERC CIP Compliance, Regulatory Services	American Electric Power 1 Riverside Plaza, Columbus, OH 43215	614-716-2351 gsfreese@aep.com	Gerald Freese is the Director of NERC CIP compliance and former Director of IT Security Engineering at American Electric Power. In his security role he was responsible for defining, developing and executing all information security programs to effectively protect AEP data and systems, including critical digital control systems. In his current capacity he is responsible for regulatory compliance, NERC CIP standards compliance and is actively engaged in development of cyber security standards for the energy industry. Gerald Freese is a recognized information security and critical infrastructure protection expert who brings a powerful combination of leadership, domain experience, technological vision and strategy development to American Electric Power. He is one of the company's primary compliance program architects, and a strong proponent of

Project 2008-06 Standard Drafting Team Roster

			industry and government partnerships for critical infrastructure protection. Prior to accepting a position at American Electric Power, Mr. Freese was the Director of Security Intelligence at Vigilinx, Inc., where he developed an early warning and data analysis process to identify computer-based threats and attack profiles. He has authored in depth analytical papers on cyber-activities relative to geopolitical and critical infrastructure threat environments, has testified before congress on critical infrastructure interdependencies and control system security and was the recipient of the 2009 'Security Seven' award for the electricity sector. Mr. Freese is a retired naval Cryptologic Officer with extensive experience in computer security and information warfare. He has held other leadership positions in the information technology industry with Perot Systems and General Dynamics Advanced Information Systems. Mr Freese is a Certified Information Systems Security Professional (CISSP). He holds a bachelors degree from State University of New York (Albany), and a Masters degree in Information and Telecommunications Systems from Johns Hopkins University in Baltimore, Maryland. He is a member of the NERC Critical Infrastructure Protection Committee, the FERC Order 706 Standards Drafting Team and is the Vice Chair of the recently formed Electricity Sector, Information Sharing Task Force. (ES-ISTF) He also participated on the Infrastructure Working Group with the Center for Strategic and International Studies (CSIS) Commission on Cyber security for the 44th Presidency.
Christine Hasha, Senior Compliance Analyst	Electric Reliability Council of Texas, Inc. 2705 W. Lake Dr. Taylor TX 76574	(512) 248-3909 chasha@ercot.com	Christine is a current member of Project 2008-06 Standards Drafting Team and has participated in other SDT project sub-teams. She is actively involved with the ERCOT CIP Working Group and participates on CIP

Project 2008-06 Standard Drafting Team Roster

			related issues for the ISO/RTO Council Standards Review Committee. Christine brings 20 years' experience in Information Technology with a 17 year emphasis on Information Security and regulatory compliance. She has provided standards training to ERCOT and other NERC region committees and has had guest speaker engagements for industry vendors. She has extensive experience in development of security policies, standards, and supporting procedures. Christine has been responsible for coordination of CIP implementation, audit readiness, and training of SMEs at ERCOT as well as representing ERCOT in CMEP related activities. She brings experience and training in common control frameworks including previous experience in implementing security controls for banking, Sarbanes-Oxley, GLBA, and HIPAA consistent with IS027001/27002.
Philip Huff Director of IT Security and Compliance	Arkansas Electric Cooperative Corporation 1 Cooperative Way Little Rock, AR 72119	501-570-2444 philip.huff@aecc.com	Philip Huff has ten year's experience in the electric industry programming and securing control systems. He has degrees in Mathematics and Computer Science from Harding University and a Masters in Computer Security from James Madison University. He is a CISSP and holds the Department of Defense certifications, CNSSI 4011, 4012 and 4014 for securing national defense systems.
Douglas D. Johnson, Principal Engineer	Exelon 1N301 Swift Road, Lombard, IL 60148	630-691-4593 douglas.johnson@comed.com	Douglas Johnson received a bachelor degree in Electrical Engineering and has worked at Commonwealth Edison - Exelon for over 29 years. He began his career in construction start-up testing and maintenance of nuclear generating plant electrical systems which included work on protective relays, main generators, large power transformers and high voltage switchyard equipment. Doug is currently part of the ComEd Transmission Operations Support organization with responsibilities overseeing the ComEd transmission dispatcher related SCADA, physical security and other communication systems. Doug has also been involved in Exelon's CIP compliance efforts since NERC

Project 2008-06 Standard Drafting Team Roster

			Urgent Action 1200 and has remained heavily involved throughout the implementation of the NERC CIP Cyber Security Standards.
Richard Kinas Manager of Standards Compliance	Orlando Utilities Commission 6113 Pershing Avenue Orlando, FL 32822	(407) 434-4261 rkinas@ouc.com	Richard Kinas is the Manager of Standards Compliance for Orlando Utilities Commission (OUC), a vertically integrated municipal utility within the FRCC region. Mr. Kinas has an undergraduate degree in Electrical Engineering and a Masters degree in Business Administration. He is a registered CISSP, and has been a NERC certified System Operator (Reliability Coordinator). Mr. Kinas has over 25 years of experience as a network and computer security expert, five of which were as a Senior Unix Administrator, five as a Senior Network Engineer, and five as a Network Security specialist. His current responsibilities include ensuring compliance with all O&P and CIP requirements for OUC. Mr. Kinas currently serves on the NERC Operating Committee, is a member of the FERC Order 706 Cyber Security standard drafting team, is the chair of the FRCC Compliance Committee, and is the vice chair of the FRCC Critical Infrastructure Protection subcommittee.
John Lim			John Lim is currently retired, since July 2012, from Consolidated Edison Co. of New York, Inc., an Electric, Gas and Steam Utility serving the New York City and Westchester County in New York. In his career at Consolidated Edison, John's most current position was Department Manager for IT Infrastructure Planning where he had overall responsibility for the enterprise cyber security program. He is an IT practitioner for more than 29 years, with more than 17 years in network and systems security in the electric utility industry. John has served as a member of the NERC Critical Infrastructure Protection Committee, as the primary cyber security representative for the Northeast Power Coordinating Council and has been active in many NERC cyber security task forces and working groups. A

Project 2008-06 Standard Drafting Team Roster

			member of the original NERC Cyber Security Standards Drafting Team, John is the current chair of the NERC Cyber Security Standards Drafting Team for Order 706. John also served as a member of the core drafting team for the DoE Risk Management Process Guideline and has served as a co-Vice-Chair of the SmartGrid Cyber Security Working Group of the SmartGrid Interoperability Panel (SGIP). He has also served as an IEEE technical paper reviewer for cyber security related to the Power sector and contributed to the EEI Reliability Newsletter. He is a frequent public speaker on cyber security for the electric sector. John holds an MS in Computer Systems from Baruch College, CUNY and is a Certified Information Systems Security Professional (CISSP) since 2001.
Robert Preston Lloyd Senior Technical Specialist	Southern California Edison 3 Innovation Village, 2nd Floor Pomona, CA 91768	909-274-1338 robert.lloyd@sce.com	Robert Preston Lloyd is a Senior Technical Specialist at Southern California Edison (SCE). He has over eight years of diverse experience in the electric utility industry involving circuit breakers, transformers, protective relays, automation systems, equipment reliability and risk assessment, asset management, General Rate Cases, compliance audits, process development, and standards development and implementation. Additionally, Robert has been involved in cyber security with SCE's NERC CIP Compliance Team for several years and has spent over two years with the NERC CIP Cyber Security Order 706 Standard Drafting Team. Robert is currently responsible for Substation Compliance & Asset Management. His involvement in compliance and regulatory issues includes NERC Protective Relays and Controls (PRC), NERC Critical Infrastructure Protection (CIP), Western Electricity Coordinating Council (WECC) Transmission Maintenance standards, California Independent System Operator (CAISO)

Project 2008-06 Standard Drafting Team Roster

			Compliance, State and Federal SF_6 Regulations, and various other regulatory bodies. Robert received both his Bachelor of Science in Electrical Engineering and his Master of Science in Engineering Management from the University of Southern California. He is also a licensed Professional Engineer in Electrical Engineering - Power.
Scott Mix CIP Technical Manager	North American Electric Reliability Corporation 1325 G Street NW, Suite 600 Washington, DC 20005	215-853-8204 scott.mix@nerc.net	Mr. Scott R. Mix, CISSP, joined NERC in October 2006 following more than 25 years of experience working in various facets of the electricity industry, including as a consultant with KEMA, Inc., Infrastructure Security Manager with the Electric Power Research Institute (EPRI), Senior Security Analyst at the PJM Interconnection, and more than ten years with Leeds & Northrup Co. as a programmer/analyst and systems architect. For more than ten years, he has focused on the areas of Computer and Infrastructure Security for the Electricity Sector. At NERC, he is responsible for Critical Infrastructure Protection issues, primarily as they relate to Real Time and Control System Security, and the development of the revisions to the NERC CIP Standards. He has also been the NERC Staff Facilitator for the Critical Infrastructure Protection Committee (CIPC) and several of its working groups and task forces, and a member of the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) Staff. Throughout his career, Mr. Mix has worked closely with numerous industry and government organizations, including NERC's Critical Infrastructure Protection Committee (CIPC) and its working teams, and is the former convener of the Control System Security Working Group, has been an active and vocal observer to the NERC Cyber Security Standards Version 1 Drafting Team (and the NERC 1200 process before that), and

Project 2008-06 Standard Drafting Team Roster

			is a former member of the OASIS "How" Working Group. He has also worked with the Department of Energy, the Department of Homeland Security, the FBI's National Infrastructure Protection Center, and the Federal Energy Regulatory Commission dealing with specific Electric Sector Security Issues. He has organized and presented at numerous industry symposia, both domestically and internationally. He has been a member and chapter secretary of the Philadelphia Chapter of InfraGard, is a member of the ISA and has participated in the ISA100 standards activities, and is a member of the IEEE as well as its Computer Society, Power Engineering Society, and Standards Association. He is a Certified Information Systems Security Professional (CISSP). Mr. Mix is a graduate of the Bloomsburg University of Pennsylvania with a Bachelor of Science degree in Computer & Information Science and Chemistry.
David S. Revill Manager, Cyber Security Operations	Georgia Transmission Corporation 2100 East Exchange Place Tucker, GA 30084	770-270-7815 david.revill@gatrans.com	David Revill is the Manager of Cyber Security Operations for Georgia Transmission Corporation with responsibility for the cyber and physical security of GTC's field assets, including compliance with the NERC CIP Standards. He previously was the Group Lead for the Electronic Maintenance lab at GTC, which was responsible for the SCADA, Revenue Metering, and Communications at GTC's field assets. Prior to joining GTC, Mr. Revill held positions supporting SCADA/EMS systems for control centers as a SCADA Systems Support Engineer and a Process Controls Network Engineer with Entergy. Mr. Revill is a member of the leadership team for the North American Transmission Forum Security Practices Group, the NERC Critical Infrastructure Protection Committee (CIPC) representing NRECA, the SERC CIPC, and

Project 2008-06 Standard Drafting Team Roster

			has been a member of the NERC CIP Standards Drafting Team beginning with version 2 of the CIP Standards. Mr. Revill holds a Master's degree in Electrical and Computer Engineering from Georgia Tech and dual bachelor's degrees in Electrical Engineering and Computer Engineering from the Tulane University.
Kevin Sherlin, IT Director	Sacramento Municipal Utility District 6201 S Street Sacramento, CA 95817-1899	(916) 732-6452 Kevin.Sherlin@smud.org	Kevin Sherlin is the Director of Information Technology at the Sacramento Municipal Utility District (SMUD), a position he has held since April, 2010. In his position as IT Director, he is responsible for all facets of information technology, including information security, leading a team of 165 skilled individuals. His previous position at SMUD was the Manager of IT Operations where he led a workforce providing IT infrastructure (PC's, servers, network, telephones, etc.). Kevin has been with the SMUD for seven years and also served as a Supervisor of Telecommunications Engineering. Prior to joining SMUD, Kevin worked at El Paso Electric Company for 24 years. He held various positions including Substation Engineer, Communications Engineer, Manager of Relay/Communications and IT Director. Kevin is a graduate of the University of Texas at El Paso with bachelor's degrees in math and electrical engineering.
Thomas W. Stevenson, Business Manager, Electric Power Industry, NERC CIP Compliance	TAI Engineering 11155 Dolfield Boulevard, Suite 210, Owings Mills, MD 21117	(410)-227-3728 or (410)-356-3108x430 thomas.stevenson@taiengineering.com	Mr. Stevenson has over forty years experience as an Electrical & Controls system engineer and project manager in the power industry. A graduate of Virginia Tech with a BS Electrical Engineering degree and George Washington University with a MS Business Administration degree, he recently retired as General Supervisor for Electrical & Control Systems Engineering in the Technical Services division of Constellation Energy. He has worked on the E&C systems design for new and existing power plants in 9 US states, Canada and Guatemala. He served as Baltimore Section President and as a

Project 2008-06 Standard Drafting Team Roster

			Certification Board member for ISA (the International Automation Society). In the ISA Power Division he has regularly served as Session Developer, Executive Committee member, Professional Development chair, and as a member of the ISA77 power plant standards committee. He is a senior member of ISA and an IEEE member since 1971. Tom has served for the last two years as a member of the NERC CIP Standard Drafting Team.
John D. Varnell Director, Market Design and Standards	Tenaska Power Services Co. 1701 E. Lamar Blvd. Arlington, TX 76006	(817)462-1037 jvarnell@tnsk.com	John Varnell has more than 30 years of experience in IT protection and control, communications systems and network security for power plants and substations. His current work for Tenaska Power Services Co., Tenaska's power marketing affiliate, includes market design and standard aspect that affect costumers in ERCOT, MISO, PJM, SERC, WECC and SPP. Mr. Varnell has served on drafting teams for NERC Project 2008-06, Cyber Security Order 706, SAR 1300 and SDT 1300, which became CIP-002 through CIP-009, Version 1, and the NERC Functional Model Advisory Team for Demand Response. He has experience with several SCADA systems, including Ferranti International Controls' Vanguard system with RealMax add-on, ESCA's Habitat System, Siemens' Spectrum System, the ABB Ranger System, OSI International Monarch System and OSIsoft PI System. He also has experience with microwave communications systems for Harris Farinon digital radios (2 and 6 GB) and Rockwell Collins analog radios (6 GB); RTU equipment, relays and interfaces from GETAC, Ferranti, Telvent, Novatech, GE, Larscom, RFL and Schweitzer Engineering Laboratory; and special systems designed in-house for gas flow computers and their interfaces and one-off embedded devices.
William Winters IT Security Architect	Arizona Public Service 400 N 5th St Phoenix, AZ 85004	602-250-4472 william.winters@aps.com	William Winters is presently an IT Security Architect with Arizona Public Service Company (APS). He has worked in the IT industry for over 30 years and has previously held positions as an IT system operator,

Project 2008-06 Standard Drafting Team Roster

			systems programmer, systems engineer and IT manager. Over the past 27 years at APS, he has been responsible for EMS/SCADA, Distribution Outage Management Systems, and other grid operations critical applications, both as an implementer and as manager. He was responsible for implementing one of the first hot multi-site distributed SCADA installations in the industry and was the CIP Program Manager for the initial implementation of the CIP Compliance Program at APS. Currently William provides enterprise security architecture direction with a focus on advancing and integrating cyber security practices across the operations and business environments.

Exhibit D

Consideration of Comments Reports

Project 2008-06
Cyber Security Order 706 Version 5 CIP Standards

Related Files

Activity: Version 5 CIP Standards (Phase III)

Status:
The Version 5 CIP Standards (CIP-002-5 through CIP-009-5, CIP-010-1, and CIP-011-1, the associated implementation plan, and the associated definitions) were approved by the NERC Board of Trustees on November 26, 2012, and they are being prepared for filing with applicable regulatory authorities.

Draft	Action	Dates	Results	Consideration of Comments
Draft 4 CIP-002-5 Clean | Redline to Last Posted CIP-003-5 Clean | Redline to Last Posted CIP-004-5 Clean | Redline to Last Posted CIP-005-5 Clean | Redline to Last Posted CIP-006-5 Clean | Redline to Last Posted CIP-007-5	Recirculation Ballots and Non-binding Poll Info>> Vote>>	10/26/12 - 11/05/12 (Closed) Non-binding Poll Extended until 11/13/12 (closed)	Summary>> Ballot Results: CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions ------- Summary>> Non-Binding Poll	

Clean | Redline to Last Posted			Results	
CIP-008-5 Clean | Redline to Last Posted CIP-009-5 Clean | Redline to Last Posted CIP-010-1 Clean | Redline to Last Posted CIP-011-1 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted Definitions Clean | Redline to Last Posted **Supporting Materials:** VRF and VSL Comment Form (Word) VRFs/VSLs for all Standards Clean | Redline to Last Posted Mapping Document Clean	VRF and VSL Comment Form Info>> Submit Comments>>	10/26/12 - 11/05/12 (Closed)		

CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Draft Consideration of Issues and Directives Clean Consideration of Comments				
Draft 3 - Version 5 CIP Standards CIP-002-5 Clean | Redline to Last Posted (CIP-002-5: REVISED 092112) CIP-003-5 Clean | Redline to Last Posted (CIP-003-5: REVISED 09/14/12) CIP-004-5 Clean | Redline to Last Posted CIP-005-5	Successive Ballot Info>> Vote>>	10/01/12 - 10/10/12 (closed)	Summary>> Ballot Results: CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions	
	CIP-006-5 RSAW Industry	09/11/12 - 10/10/12 (closed)		

Clean | Redline to Last Posted CIP-006-5 Clean | Redline to Last Posted CIP-007-5 Clean | Redline to Last Posted	Comment Period RSAW Feedback Form>> Please send RSAW Feedback Forms to: RSAWFeedback@nerc.net			
CIP-008-5 Clean | Redline to Last Posted CIP-009-5 Clean | Redline to Last Posted CIP-010-1 Clean | Redline to Last Posted CIP-011-1 Clean | Redline to Last Posted Implementation Plan Clean | Redline to Last Posted (Implementation Plan: REVISED 09/17/12) Definitions Clean | Redline to Last Posted (Definitions: REVISED 09/21/12)	Standard Comment Period Info>> Submit Comments>>	09/11/12 - 10/10/12 (closed)	Comments Received>>	Consideration of Comments **(5)**

Supporting Materials: Unofficial Comment Form (Word) VRFs/VSLs for all Standards Clean | Redline to Last Posted Mapping Document Clean | Redline CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 **Consideration of Comments** Consideration of Comments A CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B CIP-004 through CIP-007 Consideration of				

Comments C CIP-008 through CIP-011 Consideration of Comments D Definitions and Implementation Plans Draft Consideration of Issues and Directives Clean | Redline				
Draft 2 - Version 5 CIP Standards CIP-002-5 Clean | Redline CIP-003-5 Clean | Redline CIP-004-5 Clean | Redline CIP-005-5 Clean | Redline CIP-006-5 Clean | Redline CIP-007-5 Clean | Redline CIP-008-5 Clean | Redline	Successive Ballot Updated Info>> Info>> Request for Additional Clarity Form>> Posted Requests for Additional Clarity>> Vote>>	05/11/12 - 05/21/12 (closed)	Summary>>(updated) Ballot Results: (Updated) CIP-002-5 CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions	
	Formal Comment Period	04/12/12 - 05/21/12	Comments Received:	**Consideration of Comments** Consideration of

CIP-009-5 Clean | Redline CIP-010-1 Clean | Redline CIP-011-1 (CIP-011-1: REVISED - 05/09/12) Clean | Redline Implementation Plan Clean | Redline Definitions Clean | Redline Clean and redline definitions documents updated on April 12, 2012 to reflect correct dates in the footer sections. **Supporting Materials** Unofficial Comment Form A - CIP-002 and CIP-003 Unofficial Comment Form B - CIP-004 through CIP-007 Unofficial Comment Form C - CIP-008 through CIP-011	Advanced Info>> **Submit Comments:** Comment Form A>> Comment Form B>> Comment Form C>> Comment Form D>>	(Closed)	Comment Form A Comment Form B Comment Form C Comment Form D	Comments A **(1)** CIP-002 and CIP-003 Includes Summary Consideration, Explanation, and Common Responses to Global Changes Consideration of Comments B **(2)** CIP-004 through CIP-007 Consideration of Comments C **(3)** CIP-008 through CIP-011 Consideration of Comments D **(4)** Definitions and Implementation Plans

Unofficial Comment Form D - Definitions and Implementation Plans Mapping Document Clean | Redline CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments Draft Consideration of Issues and Directives Clean | Redline				
CIP Standards Version 5 Webinar Slides	04/10/12			
Draft 1 - Version 5 CIP Standards CIP-002-5 CIP-003-5 (CIP-003-5: REVISED -	Initial Ballot Info>> Vote>>	12/16/11 - 01/06/12 (Closed)	Summary>> Full Record Ballot Results: CIP-002-5	
	Formal Comment	11/07/11		

11/22/11) CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 Implementation Plan Definitions **Supporting Materials** Unofficial Comment Form (Word) Mapping Document CIP-002-4 CIP-003-4 CIP-004-4 CIP-005-4a CIP-006-4c CIP-007-4 CIP-008-4 CIP-009-4 Consideration of Comments from June 2010 Informal Comment Period Draft Consideration of Issues and Directives	Period Info>> Submit Comments>>	- 01/06/12 (Closed)	CIP-003-5 CIP-004-5 CIP-005-5 CIP-006-5 CIP-007-5 CIP-008-5 CIP-009-5 CIP-010-1 CIP-011-1 CIP V5 Implementation Plan CIP V5 Definition Comments Received>> Additional Link for Comments Received_CSWG>>	
	Join Ballot Pool Info>> Join>>	11/07/11 - 12/15/11 (Closed)		

CIP Standards Version 5 Webinar Slides		08/24/2011		
CIP Standards Version 5 Presentations - August 2011 SDT Meeting		08/17/11		
CIP Standards Development Overview for FERC Technical Staff Meeting		07/28/11		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form A
CIP-002 and CIP-003 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 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

Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated

In response to draft 2 of the Version 5 CIP Cyber Security Standards, the Standards Drafting Team (SDT) received significant input from a wide variety of perspectives. All of that input greatly helped the team to refine the standards and associated documents, and the set of standards now posted reflects all of that combined input. There were several varied perspectives in the comments, and the SDT attempted to address each comment as responsively as possible.

There were several changes that reflected careful consideration of several comments that affected the standards on a global basis, whether in format, style, or substance. In addition, there were several comments the SDT considered that were repeated across multiple questions, sometimes submitted by the same entity to each or to many of the questions. Rather than explaining in detail the global changes in response to each question, and rather than responding separately to the frequently repeated comments in each question, the SDT addresses those global issues and general comments in this section.

Many comments related to specific language suggestions or to specific compliance concerns. The SDT has responded to those comments in each of the individual questions summaries that follow this section. Those comments were thorough and varied, and they reflected diverse perspectives and topics. The SDT expended considerable work in reviewing, discussing, and responding to all of these inputs, and it believes that the major issues have been addressed responsively in this posted draft CIP Version 5 package. As a result, the changes have been significant and substantive in all of the draft CIP Version 5 standards and Implementation Plan. The SDT believes this posting package addresses all of the substantive issues received from the previous two iterations of comments and various other inputs.

Change in labeling of the applicability columns in the tables to "Applicable Systems"
After posting draft 1 of CIP Version 5, commenters expressed concern that merely using "Applicability" as the title of the applicability columns in the Requirement tables (in CIP-004 through CIP-011) created confusion with the actual "Applicability" section of the standards. In response, for draft 2, the SDT added specificity and labeled those columns "Applicable BES Cyber Systems and associated Cyber Assets." In response to that change in draft 2, commenters expressed concern with the length and suggested that the SDT label the applicability column "Applicability." Therefore, the SDT is proposing to label these columns, "Applicable Systems." This should eliminate any confusion with the applicability section of the standards themselves while also providing appropriate brevity.
Handling of "associated" Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCA) (and the associated change to their use in the "Applicable Systems" column of the requirement tables)
In previous drafts, in the applicability columns (now "applicable systems" columns), the standards used a term "Associated Protected Cyber Assets," "Associated Electronic Access Control or Monitoring

Systems," and "Associated Physical Access Control Systems" where it intended that the requirement part be applicable to not only the applicable high or medium impact BES Cyber Systems, but also to other Cyber Assets or systems, as specified, associated with those BES Cyber Systems. Also, for Protected Cyber Assets, the requirement applied to Cyber Assets or lower impact BES Cyber Systems that were in the same ESP as the applicable BES Cyber System. There was confusion the precise meaning or application of the "associated" systems, and the SDT has made the link more explicit in this draft. One of the fundamental concepts of CIP Version 5 is that it is adopting a systems approach, and those "associated" systems should be more closely connected with the applicable subject of the requirement. Therefore the SDT has moved the associated systems to follow immediately after the subject of the requirement and clarified that they are "associated with" that specify type of BES Cyber System or other applicable system. Mitigation for the associated systems may be accomplished through other applicable systems.

High Watermarking Concept

The CIP Version 5 Standards use a term "Protected Cyber Assets" to refer to those Cyber Assets that are within the ESP, which in previous versions of the standards were "other (non-critical) Cyber Assets within the ESP" (see CIP-005-4, Requirement R1, Part 1.4, and CIP-007-4). Additionally, in Version 5, a Protected Cyber Asset can also be a BES Cyber System of a lower impact classification if it is within the same ESP as a higher impact BES Cyber System.

For example, CIP-005-5, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The standard does not require segmenting of BES Cyber Systems by impact classification, and many different impact classifications can be mixed within an ESP. However, all of the Cyber Assets and systems within the ESP will be elevated to the level of the highest impact BES Cyber System present in

the ESP. The standard accomplishes this by defining all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

Measures: "but not limited to"

Many commenters expressed concern about or questioned the meaning of the use of "but not limited to" in the previous draft and asked for it to be removed from the measures. The concern as the SDT understood it was that "but not limited to" could be used to request evidence beyond that which is specified in the measure even if the entity has otherwise provided what the measure describes. With respect to "but not limited to," the SDT specifically inserted that phrase to assist the Responsible Entity, particularly in light of technologies that may change. It is not intended to be used as a mechanism to request additional evidence beyond that which is required to demonstrate compliance. The SDT is concerned that removing "but not limited to" opens the same question (albeit in slightly different context) as the CIP Interpretation Drafting Team just answered with respect to the interpretation of CIP-002 (versions 1 through 4) for Duke Energy (NERC Standards Development Project 2010-INT-05). Namely, are the measures listed exhaustive/prescriptive or are they illustrative? By including a qualifier such as "but not limited to," as is common in statutory drafting and in other legal contexts, the SDT intends to signal that the measures are not exhaustive. It provides flexibility to the Responsible Entity on what is acceptable. For example and for purposes of illustration, if one said "evidence may include an orange, a lime, or a lemon," one could expect that perhaps only an orange, a lime, or a lemon would be appropriate. However, if one said, "evidence may include, but is not limited to, an orange, a lime, or a lemon," one could just as reliably expect that an orange, a lime, or a lemon would be appropriate, but it would also be reasonable that something not explicitly enumerated by the list, but similar in nature to items on the list, such as a tangerine, may also be acceptable. Importantly, that is not the same as additionally requiring a tangerine even though one already has an orange; however, that is the concern manifested in the comments. To address the commenters' concerns, however, the SDT has made a slight change in support of signaling in all measures that they are examples and that the list of examples is not exhaustive. The SDT believes that it is providing sufficient flexibility in this manner—and for the Responsible Entities' benefit—in clarifying that measures are not prescriptive lists while also attempting to allay fears that "but not limited to" will be used in a manner that expands the requirement. Rather than stating "Evidence may include, but is not limited to, . . ." the SDT has added the "example" concept to precede "evidence" (e.g., "**An example of** evidence may include, but is not limited to, . . ." or "**Examples of** evidence may include, but are not limited to, . . .").

Movement to focus on correcting deficiencies in certain requirements:
In response to several comments, the SDT has incorporated within CIP Version 5 a recognition that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain requirements. The intent is to change the basis of a violation in those requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. Where used, the requirements incorporate the forward-looking language into the main requirement, which ties in with CIP Version 5's use of accompanying tables. It is presented in those requirements as follows:

> "Each Responsible Entity shall implement**, in a manner that identifies, assesses, and corrects deficiencies,** one or more documented processes (or program, etc., as specified by the requirement) that collectively include each of the applicable items in [the referenced table]."

The SDT also considered several alternatives and additions to this language. For example, some alternatives proposed modifying "process" (or program, etc.), while others suggested to add language specifying certain things that are not violations in addition to the requirement language. Many of the ideas or suggestions presented concepts that the team agrees with, but they are more appropriate for other aspects of monitoring compliance with the standards, not for inclusion within the standards themselves. Language indicating what is not a violation is more appropriate for compliance tools such as the RSAW. The SDT also notes that the VSLs will reflect this approach where the approach is used, and the SDT is actively working with NERC Compliance Operations to prepare the RSAWs for the CIP Version 5 standards. Furthermore, the SDT expects continued participation by industry in providing input into the RSAW development following approval of the standards, and the SDT notes that a draft RSAW for part of CIP-006-5 is posted for comment and for illustrative purposes.

The SDT is charged with writing straightforward requirements stating the desired behavior that will maximize reliability of the BES. The CIP requirements are written to require documented processes that must address the elements in the tables that accompany the requirements. These tables therefore set the parameters for the processes. There are no issues with documenting the processes – the entity must have the processes and they must have the parameters as outlined in the requirement tables.

The compliance concerns, especially those related to zero tolerance for deficiencies, is not related to the documenting of the processes, but in the implementation of the processes. The process should have numerous 'bright line' parameters that outline the goal the industry striving towards. A concern applies when implementing the processes in a world of tens of thousands of people and hundreds of

thousands of Cyber Assets. In certain cases, absolute perfection forever is not reasonable, even if it is desirable.

In light of the direction toward a risk-based approach to compliance monitoring by NERC, The CIP SDT had an opportunity to do to address this issue in certain requirements within the standards themselves. As described above, the SDT included a phrase to modify the verb 'implement' in several (but not all) of the requirements in CIP V5. Entities are to have the processes; the processes must meet the requirements in the tables; and the entities shall implement those processes in a manner that identifies, assesses, and corrects deficiencies.
The emphasis of the self-correcting language is on the implementation of the processes. The processes themselves cannot miss required parts or parameters as outlined in the tables.

Implementation Plan proposal to extend Version 3 until Version 5 remains unchanged in this draft
In light of the order approving the CIP Version 4 standards (FERC Order No. 761), several commenters asked about the drafting team's proposal in the implementation plan to extend Version 3 until the effective date of Version 5. The SDT's proposal, if approved—and its intent for Version 5 to supersede Version 4 and to extend the effectiveness of Version 3 until Version 5 goes into effect—remains unchanged.
In the implementation plan for the CIP Version 5 standards, the SDT has previously proposed to extend Version 3 until the effective date of Version 5. In doing so, the effective date proposes that Version 4 will be superseded by Version 5 and not go into effect. Even though Version 4 has been approved by order, the SDT always contemplated such approval during the development of the implementation plan language. That order does not change the SDT's proposal. The expectation that there would be an order in early to mid 2012 is why the SDT included language in the implementation plan's effective date to specify that the extension of Version 3 until Version 5, and that Version 4 would not go into effect, would occur "notwithstanding any order to the contrary." There is no change in the SDT's intent and proposal to extend Version 3 until Version 5, and for Version 5 to supersede Version 4, notwithstanding the recent order approving Version 4. The SDT also understands, as is the case for any standards proposal by the industry, that the proposal is subject to approval by regulatory authorities.

Stakeholders will notice that within the individual standards for CIP Version 5, the effective dates have been modified so that they are specific to the particular standard. In doing so, the reference to extending Version 3 and superseding Version 4 has been removed, as the Implementation Plan is the appropriate place for that language (where it remains, as described above). Thus, while there is no change to the SDT's proposal, the individual, standard-by-standard effective dates have been modified to comport with the style and form of other NERC Reliability Standards.

Annual v. 15 calendar months
Several commenters expressed dissatisfaction with the standards' use of the phrase ". . . at least once every calendar year, but not to exceed 15 calendar months . . ." for describing the required frequency

of performance on some requirements. Some entities expressed a desire to simply use "annual," while others suggested changing the "but" to an "or." The SDT has discussed alternative approaches and is using the term ". . . at least once every 15 months . . ." to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. As explained in the global comment section of the response to comments for draft 2, simply using "once per calendar year" creates a potential for bi-annual bookending that the SDT does not intend. Similarly, the SDT understands that the use of both "calendar year" and "15 calendar months" was unnecessarily complicated. The SDT acknowledges that there is a CAN that addresses "annual," but that applies where the standard does not make clear what it means in its use of the term. In CIP Version 5, there is an opportunity and an obligation to unambiguously reference the periodic time parameter. Furthermore, one of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify an audit interpretation. Instead, the SDT used specific language to clarify a time parameter that approximates one year in time while also accounting for operational realities that make a 15 month parameter more reasonable. The term "annual" is no longer used in these CIP standards for periodic requirements, and, therefore, the CAN on the word "annual" can no longer apply.

TFE v. Per Cyber Asset Capability

Historically, phrases such as "where/when technically feasible" have been considered trigger language for requirements necessitating a technical feasibility exception ("TFE") in instances where a device could not meet the required parameter. The SDT has spent considerable time reviewing each use of TFE language in CIP Version 5 where it is necessary.

The SDT has also determined that there are some requirement parts that should not require a TFE, as certain parameters are not essential themselves, but should apply if a device is capable of the parameter. This is distinct from the reasoning for requirements with TFE language. In the latter requirements, a certain performance or parameter is required, regardless of technology, device, etc. By using "per (device/system) capability," the SDT does not intend that the specific parameter or performance is required regardless of capability, but only applicable on devices that have that capability. For example, proposed CIP-007-5, Requirement R4, Part 4.1 requires "Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents . . ." Here, the SDT does not intend to require event logging. However, if a Responsible Entity is using a device that can log events, it is required to enable event logging to the extent the device is capable.
The phrase "where technically feasible" indicates that the standard requires strict compliance without a TFE. As mentioned above, the drafting team does not intend for some requirements to be TFE-triggering. The underlying rationale for a TFE is that there is legacy equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[2] Under such circumstances, the responsible entity must file a TFE that demonstrates strict compliance with an

[2] Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing, Paragraph 3

applicable requirement is not technically possible and that there is an alternative course of action that will protect the reliability of the Bulk-Power System to an equal or greater degree than strict compliance.[3]

While a TFE requires an entity to show why strict compliance with an applicable requirement is not technically possible, "per device capability" clarifies that the requirement is only applicable to the devices for which compliance with a particular requirement is possible in the first instance. This provides reasonable flexibility to the industry while also retaining the TFE concept where necessary. Thus, the "per device capability" alternative reduces the need for TFEs and will be less onerous on entities. The SDT does not intend to eliminate TFEs altogether, but proposes to use the "per device capability" as an alternative that is effective in protecting the reliability of the Bulk-Power System.

VSLs

In previous drafts of the Version 5 CIP Cyber Security Standards, VSLs were posted concurrent with each standard. For this posting, the VSLs are presented in one document. They will continue to be prepared for posting for non-binding poll during the recirculation ballot. The VSLs should not be a basis for a ballot determination, and the SDT will continue to refine them as necessary.

Applicability Section of the standards (Introduction - Section 4 – Applicability)

There were several comments about the Applicability section of the standards in various comments related to specific standards. The SDT has reviewed those suggestions and made several changes to the applicability sections of each standard.

Several commenters stated that in part 4.2 of section 4, the criteria for qualified Distribution Providers and Load Serving Entities for UVLS/UFLS systems remain unclear. Specifically, the language was not clear on whether the 300 MW of load referred to the DPs and LSEs' share or to the total load shed. In addition, they also noted that the language for Transmission Protection systems is unclear and needs clarification to more precisely describe the protection systems that are in scope. They also suggested that these should be moved to Low Impact because there is no justification for small entities to be subjected to the requirements for Low and Medium entities. The SDT has proposed modified language to clarify the qualifications for UFLS and UVLS systems that specifies that they are those UFLS or UVLS systems that are part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard and that perform automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more. With regard to the impact classification, the SDT believes that because of the function that UVLS and UFLS systems play in last ditch efforts to stabilize the BES, the 300 MW threshold provides a measure of impact that justifies the classification as medium impact systems: lower impact systems have already been removed from the scope and are not subject to these standards.

[3] Id, Paragraphs 5 and 8

Many references in the applicability section use a threshold of 300 MW for UFLS and UVLS. This particular threshold of 300 MW for UVLS and UFLS was provided in Version 1 of the CIP Cyber Security Standards. The threshold remains at 300 MW since it is specifically addressing UVLS and UFLS, which are last ditch efforts to save the Bulk Electric System. A review of UFLS tolerances defined within regional reliability standards for UFLS program requirements to date indicates that the historical value of 300 MW represents an adequate and reasonable threshold value for allowable UFLS operational tolerances.

Several comments indicated that LSEs should not be included in section 4 since the NERC Functional Model does not include any tasks related to the implementation and operation of load shedding systems. The SDT reviewed the LSEs tasks in the NERC Functional Model and has removed LSEs from the applicability of the CIP standards.

Several commenters suggested that the following language be added to the end of the criterion for Protection Systems: "and where the Protection System is connected to a supervisory control system providing remote operation capability." The SDT has reviewed the proposed addition to section 4.2.2 for Protection Systems and does not believe that the additional language to restrict the scope to only those Protection Systems that are remotely operated is intended or justified in the scope of section 4.2.2. The SDT notes that the proposed addition makes the assumption that all cyber vulnerabilities are based on remote operation capability. This would provide an incomplete mitigation for cyber threats that do not rely on remote operation for execution.

Several commenters stated that the inclusion of the glossary term "Systems" does not apply to DPs as used in section 4.2.2. One comment also pointed out that this is true in many other places where the term is used, while others' comments pointed out inconsistencies in the use of the term. The SDT notes that the terms Facilities, systems and equipment is always used in combination in the context of this application. The SDT has considered the intent of the terms in its uses and agrees that the glossary term "Systems" does not reflect the intent, and the SDT has made those changes where appropriate. In addition, the SDT believes that the issue is relieved with the changes made to refer to "assets" when referring to a group of Facilities, systems or equipment at a given location.

One comment stated that the statement at the beginning of the guideline and technical basis section that refers to applicability to DPs that refer to EOP-005 should be deleted since section 4.2.2 scopes more than EOP-005. In response, the SDT notes that the paragraph also includes reference to the registration criteria, in addition to EOP-005. The SDT believes the reference is appropriate.

One comment noted that in section 4, part 4.2.2, all single points of failure in the cranking paths should be protected and that where the Blackstart Resource is outside of the Responsible Entity's ownership, that the part of the cranking path that is the injection point to the cranking path to the unit to be

started should be specified. The SDT notes that Section 4.2.2 is not the criterion for determining the protection of the cranking path, but rather defines which part of a DPs equipment is in scope.

One comment suggested additional qualification in section 4 to ensure that the exemption section covers all facilities covered under a cyber security plan under the Nuclear Regulatory Commission (NRC) regulations. The SDT agrees with the clarification and has included the suggestion in the language in section 4 that covers nuclear facilities. The language has been added to section 4.2.4.3 to read: "In nuclear plants, the Systems, structures, and components that are regulated by the NRC under a cyber security plan pursuant to 10 C.F.R. Section 73.54."

One comment discussed the use of the phrase "required by a NERC standard" in section 4 and instances of affected Facilities, systems and equipment where there is no requirement to implement them by a NERC standard. The SDT agrees with the discussion and has made modifications to the language to more accurately reflect the intent.

One comment stated that section 4.2.4.2 attempts to define exemptions for communication links, but fails to include the exclusion of end points to those circuits (see CIP-005/R1.3). The SDT notes that end-points of circuits that are access points are included by the definition of Electronic Access Points (i.e. they are not "between" ESPs).

Reason for CIP Version 5

Some commenters inquired in their comments why CIP Version 5 was necessary, or they expressed a preference to continue under existing versions of the CIP Standards. To facilitate understanding of the reasons for Version 5 as part of the obligation to address the remaining directives in FERC Order No. 706, the SDT offers the following explanation and review of the previous versions of the NERC CIP Reliability Standards.

The NERC Board of Trustees adopted the first version of the CIP Reliability Standards on May 2, 2006. On August 28, 2006, NERC submitted to FERC for approval the Version 1 CIP Reliability Standards. On January 18, 2008, FERC issued its Order No. 706. In this order, FERC approved the Version 1 CIP Reliability Standards and issued more than 100 directives to NERC that included modifying the standards. An SDT began a phased-in approach to respond to the directives in FERC Order No. 706. As part of that phased-in approach, the SDT addressed the directives in the order that it could respond to quickly, and it developed a plan to address the remaining directives.

Version 2 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on May 6, 2009. On May 22, 2009, NERC submitted to FERC for approval the Version 2 CIP Reliability Standards. On September 30, 2009 FERC issued its Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing. In this Order FERC approved the Version 2 CIP Reliability Standards and issued four additional directives to NERC that included modifying the

standards, with a required response in 90 days. At that time the SDT had to abandon it plan for addressing the outstanding directives in Order No. 706 and had to immediately address the newly issued directives.

Version 3 of the CIP Reliability Standards was adopted by the NERC Board of Trustees on December 16, 2009. On December 29, 2009, NERC submitted to FERC for approval the Version 3 CIP Reliability Standards. On March 31, 2010 FERC issued its Order on Compliance. In this Order FERC approved the Version 3 CIP Reliability Standards.

Version 4 of the CIP Reliability Standards (CIP-002-4 through CIP-009-4) was developed as an interim step to address the more immediate concerns from FERC Order No. 706, paragraph 236, especially those associated with CIP-002's identification of Critical Assets and the risk-based methodology used for the identification. CIP-002-4, which included a bright-line based approach for criteria used to identify Critical Assets in lieu of an entity defined risk-based methodology, and the conforming changes to CIP-003 through CIP-009, was approved by the Board of Trustees in January of 2011. On September 15, 2011, FERC issued a Notice of Proposed Rulemaking (RM11-11) to approve Version 4 of the Cyber Security Standards with a 60 day comment period. The Commission approved Version 4 on April 18, 2012.

Work has continued on further improvements to the standards, including responses to the remaining Commission directives from FERC Order No. 706, and it is these further enhanced standards that will be submitted to the Commission as Version 5. The next version of the CIP Reliability Standards will build on the Version 4 standards' establishment of uniform criteria for the identification of Critical Assets.

Version 5 of the CIP Reliability Standards provides a cyber security framework for the categorization and protection of BES Cyber Systems to support the reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the cyber systems needed to support Bulk Electric System reliability, and the risks to which they are exposed.

The changes in Version 5 also present many strategic advantages. Chiefly, a significant deliverable is to close out FERC Order No. 706. More importantly, Version 5 aligns to essential reliability functions and provides significant flexibility to entities in adapting requirements to individual operations.

Version 5 represents a systems-based approach to standards, which provides an opportunity to implement solutions and tailor security based on function, connectivity, risk, and impact. That flexibility represents a significant transition from the "in or out" demarcation for applying requirements in Versions 1 through 4 of the standards, as the drafting team has been able to structure Version 5 in a way that more finely tunes the applicability of each requirement based on connectivity, impact, and other characteristics.

Version 5 is also an experience-based set of standards. It is the first opportunity for the industry to evaluate, consider and incorporate lessons learned from implementation and audit of Versions 1 through 3, and the requirements aim to provide clearer emphasis on the required results. Collectively, the Version 5 standards support continued improvement in support of protecting against compromises that could lead to misoperation or instability in the Bulk Electric System.

NERC Quality Review

In addition to the changes that were made in response to comments, the SDT also submitted the set of standards to NERC for a quality review (QR). In response to the QR, the SDT made several changes for clarity, most of which related to style and form, grammar, word choice, etc.

The Applicability section was modified in response to QR to add "Interchange Authority" to the list of functional entities. The NERC Functional Model lists "Interchange Coordinator" while the registration criteria list "Interchange Authority," and they are not yet synchronized. Until that occurs, the SDT specifies that the standards apply to "Interchange Coordinator or Interchange Authority."
The SDT removed CIP-004-5, Requirement R4, Part R4.2. In previous drafts of the CIP standards (which was Requirement R6), the standard required designation of "one or more individuals" to authorize access, followed by a second requirement part for that individual to authorize based on need. The SDT has determined that the designation of one or more individuals is administrative in nature and is something that should be addressed by the Responsible Entity's plan, not by a requirement part. The performance required is now addressed through one requirement part.

The SDT also removed CIP-006, Requirement R3, Part R3.2, which required that Responsible Entities document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 calendar months. This requirement was a documentation requirement, and the SDT, in adding the modifying language to "identify, assess, and correct deficiencies" to Requirement R1, determined that the documentation requirement to log outages was not necessary.

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.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10

7.	Rick Crinklaw	Lane Electric Cooperative	WECC	3
8.	Annie Terracciano	Northern Lights Inc.	WECC	3
9.	Aleka Scott	PNGC	WECC	4
10.	Heber Carpenter	Raft River Electric Cooperative	WECC	3
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC	1, 3
12.	Marc Farmer	West Oregon Electric Cooperative	WECC	4
13.	Margaret Ryan	PNGC	WECC	8

12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14.	Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	M & A Electric Power Cooperative	SERC	1, 3	
4.	Northeast Missouri Electric Power Cooperative	SERC	1, 3	
5.	N.W. Electric Power Cooperative, Inc.	SERC	1, 3	
6.	Sho-Me Power Electric Cooperative	SERC	1, 3	

15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Oglethorpe Power Corporation		SERC	5
2.	Georgia Transmission Corporation		SERC	1

16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWERENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
8.	SCOTT NICKELS	RPU	MRO	4
9.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
10.	MARIE KNOX	MISO	MRO	2
11.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
12.	SCOTT BOS	MPW	MRO	6, 1, 3, 5
13.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
14.	THERESA ALLARD	MPC	MRO	1, 3, 5, 6

17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	James Howard	Lakeland Electric	FRCC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Darl Shimko	MGE	MRO	3
2.	Joseph DePoorter	MGE	MRO	4
3.	Steve Schultz	MGE	MRO	5
4.	Jeff Keebler	MGE	MRO	6

20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Jones	Pepco	RFC	1

21.	Group	Rick Terrill	Luminant					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6
9.	Brenda Hampton	Luminant Energy Company LLC		

22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Smith	BANC	WECC	1

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Rayburn Country Electric Cooperative		SPP	
2. Empire District Electric		SPP	1
3. City Utilities of Springfield		SPP	4
4. Westar Energy		SPP	1, 3, 5, 6
5. Cleco Power		SPP	1, 3, 5, 6

25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						

Additional Member	Additional Organization	Region	Segment Selection
1. Pawel Krupa		WECC	1
2. Dana Wheelock		WECC	3
3. Hao Li		WECC	4

27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					

Additional Member	Additional Organization	Region	Segment Selection
1. Denise Lietz	Puget Sound Energy	WECC	1
2. Erin Apperson	Puget Sound Energy	WECC	3

28.	Group	Michael Mertz	PNM Resources	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1. Laurie Williams	Public Service Co. of New Mexico	WECC	1
2. Michael Mertz	Public Service Co. of New Mexico	WECC	3

29.	Group	Sasa Maljukan	Hydro One	X									

Additional Member	Additional Organization	Region	Segment Selection
1. David Kiguel	Hydro One	NPCC	1

30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION A3 – CIP-002-5:

If you disagree with the changes made to CIP-002-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, the SDT made significant changes to attachment 1 and provided clarity to the requirements and associated rationales and measures. The explanations below describe the modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity in language.

Introduction - Section 4 – Applicability
There were several comments on this section in response to question A3, but the issues and responses relate generally to all of the standards. The discussion and response to comments on this section is provided earlier in this document in the Summary Consideration, Explanation, and Common Responses to Global Changes and to Issues and Comments Frequently Repeated section.

Requirement R1
Substantial changes were made to both the structure and the approach in Requirement R1: while the end result is a categorized list of high and medium impact BES Cyber Systems, there were many changes made to address concerns related to Low Impact assets and an asset based approach to deriving BES Cyber Systems. Many comments suggested a more prescriptive approach to the methodology used to arrive at the objective lists, including suggestions to add a flow-chart to the requirement: the SDT made a number of changes to address the "what" instead of the "how", and added substantive qualifications to better define the assets affected.

In particular, several commenters stated that the requirement to review and update the categorization on every change to the BES was an onerous burden in a company with a large number of constantly changing BES Facility configuration. The SDT has reviewed comments and is persuaded by the arguments presented. The SDT also considers that an annual review and update for BES Facilities, given the long term implementation of BES Facility changes, together with the requirements for BES Cyber Systems change control, provide a framework that provides the controls necessary.

Several commenters stated that the requirements for identification in Requirement R1 of CIP-002-5 be modified to require reference to “BES Sites” rather than Facilities, systems and equipment. One comment also suggested that inventories for Low Impact would allow requirements for low impact to be at the site level. Many comments suggested a Facilities impact-based approach to the derivation of the impact of BES Cyber Systems. The SDT has considered the suggestion and made modifications to the current CIP-002-5 requirements to incorporate the concepts using language already used in the criteria and Version 4 approved standards. While the terms Facilities, systems and equipment are precisely the same terms used in the definition of Critical Assets in prior versions, the SDT has made modifications to the proposed language to use the term “assets”, a term familiar to the industry in compliance activities for prior versions.

In response to numerous comments on the issue of asset-based derivation of cyber system impact, the SDT made substantive changes to Requirement R1s language and structure to include this approach. While Requirement R1 is ultimately intended to result in categorized BES Cyber Systems for the application of cyber security requirements, the SDT has made changes to the language and contents of Requirement R1 as well as the criteria in attachment 1 in consideration of comments received.

Several commenters commented on the use of the capitalized term Bulk Power in the rationale for Requirement R1. The paragraph has been deleted and the term is no longer used in the rationale.

One commenter suggested that a bullet is not required in requirement part 1.3 of Requirement R1. The comment also suggested an inconsistency between Requirement R1 and the associated VSL. The SDT has redrafted Requirement R1 in consideration of comments and the bulleted clause is now in the applicable part of the requirement. The inconsistency in the VSL has been corrected.

One commenter suggested that the SDT continues to insist there is no need to identify the low impact BES Cyber Systems and their associated Cyber Assets (e.g., R1.3) and that this causes an auditability issue. The SDT believes that an “asset” based approach in the revised draft and the requirement for the list of assets containing Low Impact BES Cyber Systems provides relief to the auditing issue.

Several commenters requested an explanation of the values used in the VSLs for Requirement R1. The SDT notes that the values are based on FERC Guidelines for VSLs that use percentages. Many entities commented on the need for absolute values for smaller entities since percentages would provide an unfair bias for small entities that would more easily reach percent based thresholds.

One comment stated that the SDT should consider reusing lists generated by other standards. The SDT notes that evidence used for other reliability standards can be presented for these CIP standards as long as they provide the evidence required to demonstrate compliance to the CIP requirement.

One commenter suggested that requirement parts 1.1, 1.2 and 1.3 should also include documentation as part of the requirement and that requirement part 1.4 should require the update prior to commissioning. The SDT's approach to requirement definition focuses on results and believes that a requirement to "document" does not directly result in the reliable operation of the BES. The SDT has defined the required functional result that directly contributes to the reliable operation of the BES. Requirement R1.4 has been removed by SDT in consideration of comments received.

One commenter suggested that by specifying requirements for Low Impact, CIP-002-5 implies a list of BES Cyber Systems. The commenter further suggested either requiring a list of Low Impact Cyber Systems or removing Low Impact altogether. The SDT notes that requirements must be explicit and that CIP-002-5 has made it clear and explicit that a list of Low Impact BES Cyber Systems is not required. However, in the new draft, a list of Low Impact assets is required to facilitate the application of policy requirements to Low Impact assets.

Several commenters suggested many editorial changes to the language used in Requirement R1. The SDT has made fundamental structural and language changes to Requirement R1 to address comments received.

Requirement R2

One commenter suggested that the rationale for Requirement R2 does not include approval of the lists. The SDT notes that the last sentence in the rationale refers to the approval process.

One commenter made many remarks on inconsistencies between the Requirement R2 language, the measure and the VSLs. The SDT has made modifications to R2 and its measures and VSLs for consistency.

Many commenters suggested alternative language, or reverting to the use of the term annual for the clause describing the annual review and approval. One commenter also inquired as to whether the clause supersedes an entity's definition of annual. The SDT has discussed alternative approaches and is using the term "at least once every 15 months" to provide reasonable flexibility to Responsible Entities while meeting the intent of the requirements. The SDT has intentionally not used the word "annual". This term is no longer used in these CIP standards for periodic requirements

and therefore, the CAN on the word annual can no longer apply in this requirement. One of the objectives of the SDT in Version 5 is to consider applicable CANs and use language that would no longer require a CAN to clarify audit interpretation. Instead, the SDT used specific language that implements its intent. This topic is also discussed in greater detail in the introductory, global section of these comment responses.

Attachment 1

Section 1 - High Impact Control Centers

One commenter stated that criteria for control centers fail to consider inter-Control Center connectivity and that the concept of mutual distrust does not work because of trusted paths. The SDT has included consideration of connectivity in the application of requirements. The applicability of mutual distrust depends on specific considerations of network configuration. A blanket statement based on an assumed configuration does not support the generalized comment. The SDT believes that requirements in the standards for protection of BES Cyber Systems provide a basis for Responsible Entities to implement the necessary protection in their network and system design.

Several commenters stated that the introductory text in High and Medium Impact criteria should be deleted or modified due to the change in approach for facilities based impact. The SDT notes that Requirement R1 still requires, ultimately, the categorization of BES Cyber Systems for the application of requirements. The SDT believes that the introductory text in the criteria for High and Medium is still required to express this result.

One commenter suggested on the inclusion of “associated data centers” in the control center criteria and argued that the BES Cyber Systems in these “data centers” would already be included. The SDT has made revisions to the definition of Control Centers, has now included data centers in the definition, and removed the phrase from attachment 1.

Many comments were received on the relationship of TO Control Centers and the functional obligations of TOPs. There was also a comment on the section in the guidance that pertains to TO Control Centers that perform the functional obligations of the TOP. In particular, one comment suggested removal of the guidance, citing ownership issues and issues with NERC Functional Entity registration. The SDT believes that the criterion in question is used to determine the impact of the BES Cyber Systems, and that, irrespective of registration issues, if these Cyber Systems perform a function that is relevant to the functional obligation of a TOP, and that this is formally delegated, then the impact should be appropriately assessed as such. The issue of ownership is a non-issue since the responsibility for compliance to the applicable requirements resides with the owner of the identified BES Cyber Systems that provide that function.

Several commenters suggested that the language used in criterion 1.3 with respect to TOP Control Centers needed clarification and that the guidance for this criterion should explicitly say that TO Control Centers that do not perform the functional obligation of the TOP should be classified as Medium. The SDT has inserted additional guidance to clarify this point. A TO facility that does not perform or does not have an obligation to perform any of the reliability tasks of a BA, TOP or GOP does not meet the definition of a Control Center and the BES Cyber Systems should be evaluated according to the criteria in attachment 1. TOs should review the functional tasks of a TOP and those of a TO and ensure they are not delegated any of these functional tasks through an agreement or a contract. In particular, TOs should note that the functional model does not list real-time operational tasks for that entity.

One commenter asked whether a TO Control Center that performs an operation under the direction of a TOP is performing a functional obligation of a TOP. The NERC Functional Model does not include operation of BES Facilities under the tasks or obligations of a TO, but does include them under the obligations of a TOP. If the TO has an obligation (contractually or because of some other formal agreement) to operate BES assets, whether it is in an emergency or in normal operational circumstances, under the direction of a TOP, then that Cyber System is used to perform the functional obligation of a TOP. The functional obligation of operational control of the BES asset has been delegated to the TO.

One commenter also asked whether a TO data center that collects data and then processes that data for transmission to the TOP is performing a functional obligation of the TOP. The SDT has moved the data center association to the definition of a Control Center and associates it with the facility hosting the operating personnel. In the scenario described, the TO data center is not associated with the BES Cyber Systems owned by the TOP. The “data center” described is analogous to field data aggregating facilities and are evaluated as BES Cyber Systems necessary for providing situation awareness for real-time operations, and should not be evaluated as TOP Control Center “data centers”.

One commenter suggested a number of modifications to the criteria aimed at better stratifying the distinction of Medium from High Impact, especially in the case of BA and TOP Control Centers. The SDT considered the suggestions and has made a number of modifications to address the comments. On another suggestion of increasing the threshold for High Impact BA and GOP Control Centers to 3000 MW, the SDT notes that the stratification of the High Impact from Medium Impact is mostly based on impact due to the wide area reliability tasks of the Functional Entities. However, the SDT has included modifications that provide some stratification of the levels for BA, TOP and GOP Control Centers which are consistent with thresholds approved in Version 4. On the subject of UFLS thresholds, the SDT reviewed recent developments in Regional Standards for UFLS and the tolerances specified in these standards as a basis for evaluation of

the current threshold: the SDT concluded that the current threshold represents a reasonable representation of the level of tolerance in these standards so far.

Several commenters suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

One commenter suggested that the word "control" in the definition of Control Center requires more explanation and that the situation awareness section of the guidelines on BES Reliability Operating Services could include cyber systems used in collecting data for management and engineering analysis. The SDT has provided, in the guideline, the type of operations included in the use of the word. The definition provides further qualification in the context of the Control Center. The word "control" is used in several other standards and is a well understood concept in the BES environment. The intent of the situation awareness section in the guideline on BES Reliability Operating Services is to broadly define a reliability function and is not meant to be used solely for the qualification of applicable BES Cyber Systems: it is intended to be a first step in qualifying a population of Cyber Systems for further application of additional qualifications in the definition of BES Cyber Systems, applicable assets and the impact criteria in attachment 1.

One commenter stated that criteria 1.2 and 1.4 in attachment 1 qualify assets affected as "generation assets" and pointed out that not all assets in scope are strictly "generation assets". The SDT agrees and has made the suggested modification.

One commenter requested clarification on whether the 1500 MW in requirement parts 1.2 and 1.4 of attachment 1 referred to criterion 2.1. The SDT responds that the 1500 MW refers to total aggregate generation of 1500 MW, and is not tied to criterion 2.1.

Section 2 - Medium Impact

Several commenters stated that the 15 minute criterion in requirement part 2.1 of attachment 1 is unnecessary and redundant. Another commenter stated that this 15 minute clause was contrary to the "bright-line" concept. One commenter also stated that the inclusion of the 15 minute qualification in the criteria was inappropriate because the criteria define BES asset impact. The addition of this qualification resulted from previous comments and sought to

provide clarity in the scope of BES Cyber Systems to be included in consideration of this criterion. Where the qualification is included, the language makes it clear that it applies to the effect of the BES Cyber System.

There was a comment that the 15 minute in criterion 2.1 and 2.2 is going to be difficult to prove in an audit and suggested the term "that operate the reactive resource" instead in 2.2. As stated in the guideline, the intent of the 15 minute is to provide a boundary to the impact to real-time operations. The alternative use of the term "real-time" does not provide a useful defined term. The SDT believes that the commenter's suggestion to use the term "that operate" in criterion 2.2 restricts the full scope of cyber systems that affect the real-time operation of the BES for reactive resources.

The commenter further suggested that criterion 2.1 should consider regional operational conditions and requested clarification on the 1000 MVAR threshold for 2.2. For 2.1, the SDT considered regional variations in determining this threshold and notes that this is the approved Version 4 criterion. For 2.2, the SDT consulted with operational and planning experts during the development of this criterion in Version 4.

One commenter stated that the commas around the words "as necessary" in criterion 2.3 were confusing. The SDT has reviewed the criterion and agrees that the commas are misplaced and have altered the intent of the criterion. The SDT has made changes to the placement of the commas to clarify the intent.

One commenter requested clarification on the use of the phrase "long term planning horizon" in criterion 2.3. The SDT notes that criterion 2.3 of attachment 1 does not use the phrase "long term planning horizon" but uses a specified one year or more near-term timeframe. The SDT notes the intent is to avoid the identification of generation facilities that could be used to remediate short term reliability issues.

Two commenters requested additional clarification in the notifications to asset owners in criteria 2.3 and 2.6. For 2.3, the notification is affected as part of the execution of a contract. For 2.6, the applicable IROL reliability standards require that the asset owners be notified. These standards do not specify how the notification is to be done, but that notification must be performed.

One commenter suggested that in requirement part 2.2 of attachment 1, the nameplate value should be qualified to account for ranges. The SDT has included a qualification of "maximum" in the criterion.

One commenter stated that criterion 2.3 references the long term planning horizon, contrary to the real-time operations aspect of the CIP standards. In addition, the commenter suggested that additional guidance be provided as to the notification of such obligations. Also, the commenter requested similar clarification in the guideline for criterion 2.8. The SDT points out that the criterion states that the designation of the asset is performed as part of a planning activity that has a time horizon of one year or more (near-term) by the Planning Coordinator or Transmission Planner, but the impact of a compromise of an affected BES Cyber System would meet the qualification for real-time operations. Additional clarification on notifications has been added to the guideline for criteria 2.3 and 2.8.

One commenter stated that the guidance section that refers to the category D contingency of TPL standards in the discussion of criterion 2.3 is unlikely and suggests removing it. The SDT has removed the reference in the guideline.

One commenter suggested using the phrase "generation interconnection facility" instead of "Transmission Facilities providing the generation interconnection required to connect generator output to the Transmission Systems Transmission Facilities" in criterion 2.8, citing the term used in Project 2010-07. Another commenter suggested on the exclusion of generation plant collector buses in criterion 2.4 and 2.5 in the guidance and suggested an explicit exclusion in the requirement. The SDT reviewed the standards in Project 2010-07 and has not found "generation interconnection facility" as a defined term in the NERC Glossary. The term is however used in the PRC standard in the project. The SDT intends that the application of this criterion to Transmission Owner/Transmission Operator owned and generator owned Transmission Facilities that provide this interconnection of generator output to the Transmission system. However, for clarity and to address the exclusion of these facilities in criteria 2.4 and 2.5 that one comment stated, the SDT has added this term as an inclusion in 2.8.

One commenter suggested alternative language for criterion 2.5 to clarify the application of the aggregate rating. The SDT made modifications to the language in 2.5 to clarify the application of the aggregate to the sum of applicable Transmission facilities at the station.

Many commenters suggested using, for criterion 2.6, the same language used in criteria 2.8 and 2.9. The SDT notes that in criterion 2.6, the criterion refers directly to the Facilities that make up the IROL and has used the exact language used in the IROL standards that require the identification of these specific Facilities. Criteria 2.8 and 2.9 apply to Facilities that could indirectly cause a violation or reduction of the IROLs.

Several comments were on the reasons for the removal of the WECC specific qualifications for those criteria that are based on IROLs. The SDT understands that the commenter has reconsidered its position on IROLs and that other changes in attachment 1 negate the need for any WECC specific qualification.

Several commenters requested information on the standards that require notification of asset owners for IROLs in criterion 2.6. One commenter also stated that the term Control Center is not a NERC defined term and to organize the guidelines by transmission, generation, etc. The SDT notes that the guidelines for criterion 2.6 provides information on the NERC Reliability Standard that contains these requirements (FAC-014) that require identification of these assets and notification to applicable owning Functional Entities. The term Control Center is a proposed defined term in this CIP standards package and the guidelines for criteria are organized by generation and transmission.

One commenter inquired as to why all facilities necessary for the NIPR (not just Transmission Facilities) are not included in criterion 2.7 (Nuclear Interface facilities). The SDT notes that the scope of applicability in NUC-001 is limited to transmission entities listed, which consists of registered entities.

One commenter requested clarification in the application guideline on how, in criterion 2.8, the TO would obtain information on whether generation it does not own or operate meets criterion 2.3. The SDT included additional guidance in the application guideline section.

One commenter stated that the UVLS/UFLS in criterion 2.10 that refers to the 300 MW threshold should specify the lowest rating in the last 12 months. Several commenters stated that the use of the highest MW rating in the guidelines and technical basis on UVLS/UFLS should be changed to “hourly integrated load”. The SDT has not specified the methodology used to determine the 300 MW and has deferred to the requirements of the applicable regional UFLS/UVLS standards.

One commenter stated that criterion 2.10 might imply that individual unconnected relays in a load shedding program under a common trip point would be included and suggested excluding these. The SDT believes that the qualification of a common control system addresses this concern and believes that the exclusion language has the unintended consequence of excluding individual relays irrespective of their impact.

One commenter stated that the language in criterion 2.10 which specifies “regional load shedding programs” is problematic since there is no such requirement and pointed out that PRC standards place the responsibility for

establishing UFLS programs on the Planning Coordinator. The SDT has made modifications to section 4 that pertains to load shedding and criterion 2.10 to more accurately reflect the requirements of the PRC standards.

There was a comment that for criterion 2.10, the language suggests that any compromised component that make up SPS, RAS or automated switching system is required to be protected regardless of if it has an effect on the IROL or not. The SDT notes that the current language does not imply this requirement. The current language only applies if the compromise, whether of one or more components of the SPS, RAS or automated switching system, would cause a violation of one or more IROLs or "cause a reduction of one or more IROLs".

One commenter suggested setting a threshold for Special Protection Systems for applicability of these CIP standards. The SDT notes that all Special Protection Systems, irrespective of any threshold, are designated as Critical Assets under Version 4. The SDT notes that this has been the case because of the critical function provided by Special Protection Systems in the reliable operation of the BES.

Numerous commenters stated that in part 2.11 of attachment 1, the threshold for generation Control Centers should be changed to 1500 MW for consistency with the generation threshold in other criteria in Medium Impact. One commenter also pointed out an inconsistent term in the flow chart in the guidelines and technical basis section. In the same area, another commenter commented that part 2.11 should be removed and that the specific hydro situation should be handled in the definition. The SDT's intent in 2.11 is to include as Medium all the remaining Control Centers not already classified as High, because of the functions provided by Control Centers. In defining a 300 MW threshold for generation Control Centers in 2.11, the SDT was attempting to address a situation specific to hydro-electric generation Facilities. The SDT has removed this artificial threshold in view of changes made to this criterion. Further, the SDT made modifications in the threshold in the criterion for generation Control Centers to address these comments. The inconsistency of terms used in the flowchart has been corrected.

Several entities commented on the removal in draft two of criteria for restoration resources (blackstart units and cranking paths) from the Medium category. Some were in favor of this removal while others were not. Specifically, one commenter made several comments regarding generation and cranking path restoration resources. One comment read that restoration resources should be rated as Medium Impact. In contrast, another commenter suggested that restoration resources should not be included in the scope of the application of the CIP standards because of the absence of the need for remote data communication in the event of a restoration and the exclusion of cranking path from the definition of the BES. In response, in addition to the justification provided as part of the draft two materials, the SDT has

further considered industry input and comments in the consideration of these criteria with respect to their effect on overall reliable operation of the BES and has now removed them from High or Medium Impact criteria. In response, the SDT notes that the assumption that remote access through data communications is necessary for the realization of cyber security threats represents an incomplete mitigation approach, and that the CIP standards are aimed at protecting cyber systems that would impact the real-time operation of the BES, not solely those that directly operate elements of the BES. NERC Reliability Standards that govern the operation of load shedding programs and the protection of the BES elements are other examples of such approaches.

Section 3 – Low Impact

One commenter noted that the criteria in section 3 of attachment 1 should include the phrase "not included in high or medium". The SDT has made the necessary clarification.

General Comments

One commenter suggested that the footnote regarding the effective date of Version 5 and the effective date of Version 4 should be moved to the main text of the effective date. The SDT considered moving this footnote, but believes that movement of the footnote could cause unnecessary confusion, since the effect would not be different. The footnote simply clarifies the effective language that Version 4 does not go into effect and is superseded by Version 5.

There was a comment that the varying language regarding the phrase "destroyed, degraded, or otherwise rendered unavailable" and its variations needs to be consistent. In addition, Southern Company provided additional clarification language for the cranking path criterion in Low Impact. The SDT has reviewed the uses of the term and has ensured consistency when referencing Facilities or BES Cyber Systems. The main difference is the addition of "destroyed" and "otherwise rendered unavailable" in the case of Facilities. The SDT has added the suggested clarification in criterion 3.3.

One comment was on the use of the word "would" instead of "could" in the standards and recommended the use of the prospective word "could". The SDT believes that the use of the word "would" is appropriate to describe the certain impact of a compromise due to an exploitation of vulnerability.

One commenter stated that the last paragraph on page seven leaves it up to the registered entity to determine the level of granularity when identifying the BES Cyber Systems and instructs the registered entity to take into consideration the operational environment and scope of management and raised questions of auditability in the text. The SDT notes that the background and guideline sections are only providing context to the standards. The only auditable parts of the

standards are the applicable definitions and requirements. The SDT directs the commenter to the definition of BES Cyber System for effective application of the requirements.

There was a comment on the examples for Electronic Access Control and Monitoring Systems in the background section, specifically the use of certificate authorities, security event monitoring systems and intrusion detection systems. The SDT uses the term "Certificate Authorities" as an example of the type of cyber assets owned by the Responsible Entity that would be subject to the CIP standards if it relates to a function that is used within the scope of a BES Cyber System. The SDT has used the generic term "security event monitoring systems" as a generic functional term and has specifically avoided the use of the various acronyms used to include this function. This is also true of the term "intrusion detection systems": the SDT is providing an example of the function, and the term "intrusion prevention systems" includes functions that are not within the scope of the requirements. The SDT acknowledges that intrusion prevention systems necessarily include an intrusion detection function.

One commenter suggested the inclusion of network attached storage and storage area networks in the examples for Protected Cyber Assets. Examples provided are not intended to be exhaustive lists, but are intended to provide some examples of the types of systems that could meet the requirements for the definition of Protected Cyber Assets. They are not intended to mean that all of these types of systems are necessarily Protected Cyber Assets, but are examples of systems that could be Protected Cyber Assets if they meet the definition.
SPP suggested footnoting the time horizon reference in requirements. Time Horizons are standard designations used in all requirements and is a standard requirement for all NERC standards requirements. They are required characteristics of each requirement in the same way that Violation Risk Factors are. The SDT believes that footnotes for these are not required as they are generically defined in other NERC documents.

One commenter requested clarification of the general use of transmission facility and its scope. In using terms such as "Facility" in the criteria, the SDT has made substantial changes to Requirement R1 that provides flexibility to the Responsible Entity to define what the term includes within the definition of the requirement. Requirement R1 now includes a listing of the types of assets to be considered that provides a more defined scope to the applicability of CIP-002-5 and the CIP cyber security standards. Within these, Responsible Entities have flexibility in defining the sets within these considerations for application of the criteria.

One commenter requested clarification on entities that have coordination responsibilities. The SDT notes that the table in the guidance provides guidance on those entities that have responsibilities for inter-entity coordination. In a

restoration scenario, those Responsible Entities that require inter-entity coordination to perform their functions that require such coordination have responsibility for this coordination.

One commenter pointed to an inconsistency between the title of the standard and the heading of the document. The SDT corrected the inconsistency.

One commenter stated that the NERC Functional Model does not define Functional Entities. The SDT notes that the current version of the Functional Model (Version 5) defines both Reliability Functions and the Functional Entity that performs the tasks. In addition, there are further responsibilities defined under Functional Entities which are specifically defined in relation with other Functional Entities.

A commenter requested additional guidance in the concept of BES Cyber System. The SDT has made several modifications to the guidance for the overall concept of BES Cyber System, including additional peripheral terms related to BES Cyber Systems, such as Protected Cyber Assets. The SDT believes these additional clarifications provide the additional guidance on the concepts.

There was a comment on the guidance on BES Reliability Operating Services provided for optional use by entities as an aid to scope BES Cyber Systems in the guideline section of the standards. One commenter also suggested removing the designation of Functional Entities for the BES Reliability Operating Services to minimize differing opinions. The SDT made several modifications to this section in consideration of these comments where appropriate. With respect to comments on voltage control and Distribution Providers, the Functional Model clearly lists voltage reduction in its tasks. The designation of Functional Entities is provided as guidance and resulted from comments from previous drafts. The SDT believes that this information provides additional guidance for some Responsible Entities in scoping their BES Cyber Systems.

One commenter suggested that the format of the standard is different and suggested moving the background to the end together with the guideline. The SDT has used the standard template for results based standards and is the recommended standards development format and approach.

There was a suggestion that the rationale should not be part of the standard. The rationale statements will be removed from the official filing and included as information, together with the guidance information.

Several comments were on the use of bright lines and the problem with a one size fits all approach without provisions for studies and engineering analysis and the requirement to require at least some protection for all BES assets. The SDT notes that the objective of Version 5 of the CIP standards is to provide some level of protection to all BES Cyber Systems according to the impact to the real-time operation of the BES assets they are supporting. The bright line based approach was approved by industry stakeholders and FERC as part of Version 4.

One commenter suggested the use of a more definitive term "prevent" in qualifying impact on functions in the reliable operation of the BES. In addition, there was a suggestion for an explanation of the use of the 15 minute window in the definition of BES Cyber Asset. The SDT believes that the word "prevent" does not provide a qualification for the full scope of applicability, but a subset. The intent of the SDT is to ensure that impacts also cover impairment as well as outright "prevention". An explanation of the 15 minute window is in the background section of the standard under real-time operations.

One comment suggested that the stipulation of ownership for compliance responsibility is inconsistent with PRC standards that also stipulate "operate". The SDT has consistently maintained that responsibility for compliance is the asset owner's.

There was a general comment on the application of FISMA and the NIST framework in relation to the CIP standards. The SDT notes that CIP V5 considered the NIST framework as one of the inputs to the drafting of these standards in response to FERC Order 706. The SDT did not consider FISMA requirements, but rather the NIST Risk management framework as directed by Order 706. The SDT also considered input from several other frameworks and has used those inputs in the drafting of standards that are subject to compulsory compliance and enforcement. The NIST 800-53 series is characterized as guidelines for controls, not compliance requirements.

QUESTION A10 – CIP-003-5:

If you disagree with the changes made to CIP-003-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major issues identified through the comment form with CIP-003-5 included (1) the list of low impact BES Cyber Systems for Requirement R2, (2) demonstration of policy implementation, (3) clarity of policy topics in Requirement R2, and (4) the reliability benefit of the annual review/approval of the cyber security policies as well as maintaining documentation of changes to the CIP Senior Manager and delegates.

List of Low Impact BES Cyber Systems for Requirement R2

Numerous commenters identified concerns that while the SDT intended to provide protection from discrete identification of Low Impact BES Cyber Systems, there was still significant concern that this would still be required in order to demonstrate compliance with the requirement. Additionally, commenters suggested that the object of the policy for Low Impact BES Cyber Systems should be on the facilities (or "sites") themselves and not specifically the Low Impact BES Cyber Systems. The SDT continues to believe that the identification of low impact BES Cyber Systems would not be required in order to comply with CIP-003-5 R2. However, the SDT also agrees with commenters that a facilities based approach to the low impact policy comes with a number of benefits. Among these being the creation of a reasonable level of abstraction (the facility) of which to refer to the low impact BES Cyber Systems, thus facilitating any necessary sampling during an audit, without explicitly needing a list of these cyber systems themselves. Consequently, CIP-003-5 R2 has leveraged a reference to CIP-002-5 where facilities with low impact BES Cyber Systems are identified. The SDT believes this approach will provide consistency of application of the policy for low impact BES Cyber Systems, provide a reasonable approach for audit oversight, and create additional clarity on the evidentiary expectations.

Policy Implementation

There were a number of comments that expressed issues with ambiguity in the use of the term "implement" as it relates to the cyber security policies in both CIP-003-5 R1 and R2. In reviewing this comment, the SDT noted that the obligation to "implement" the cyber security policy has existed since version 1 of the CIP standards. Additionally, FERC directed the ERO in Order 706 to "to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards." While this directive did not specifically direct changes to the cyber security policy, as this policy already had the obligation to implement in version 1, the SDT is cognizant that any change to the contrary would require reasonable justification.

As it relates to the CIP-003-5 R1 cyber security policy for medium impact and high impact BES Cyber Systems, the SDT believes there is sufficient justification to make a modification to the language of the requirement in order to provide the clarity that the industry desires around the obligation to "implement." The SDT strongly believes that it has not lessened the obligation to implement the cyber security policy. However, given the required scope of the CIP-003-5 R1 cyber security policies, the SDT believes that implementation of these cyber security policies is effectively demonstrated through compliance with CIP-004-5 through CIP-011-1. Therefore, the SDT has chosen to remove the term "implement" from CIP-003-5 R1. The SDT believes that this should provide clarity as to the expectation of implementation as well as to relieve concerns of double jeopardy between CIP-003-5 R1 and the entire body of CIP-004-5 though CIP-011-1.

The SDT has handled this concern differently for the low impact cyber security policies in CIP-003-5 R2. As there are no corresponding requirements in CIP-004-5 through CIP-011-1 that require explicit implementation of areas addressed by the low impact policy, there are no double jeopardy concerns. The SDT has attempted to provide structure around the obligation to implement the cyber security policies through the global modifications that provide for continuous improvement and the identification, assessment, and correction of deficiencies. The expectation of the SDT is that entities will define cyber security policies that address the four required areas and put these policies in effect using an overall framework that provides reasonable assurance that the policies are applied through methods that identify, assess, and correct any deficiencies.

Policy Topic Clarity for Low Impact Policy

In addition to ambiguity over the implementation of the cyber security policy for low impact BES Cyber Systems, commenters expressed concern over the clarity of the individual policy topics for low impact BES Cyber Systems. The SDT appreciates these comments and has made some modifications to the topic language. However, the SDT understands that these modifications do not completely alleviate the concerns around individual topical clarity. The SDT has modified the topic "Physical access controls" to "Physical security controls" and "Electronic access controls" to "Electronic access controls for external routable protocol connections and Dial-up Connectivity." The SDT chose to not add too much additional detail to these policy topics in recognition of the wide range of environmental, geographic, technical, operational, and logistical differences that may exist amongst the set of low impact BES Cyber Systems. As such, the SDT's intent is to allow Responsible Entities to have flexibility to design and implement the most efficacious security program possible for their particular set of low impact BES Cyber Systems. The modification to physical security controls over physical access controls acknowledges this approach. "Physical security controls" gives great discretion to the Responsible Entity to choose controls that are effective. The SDT believes the paradigm shifts in NERC CIP Reliability

standards allowing for multiple levels of security (high, medium, and low) and creating an atmosphere of continuous improvements through the identification, assessment, and correction of deficiencies will address the concerns of compliance risk that are driving the need for more prescriptiveness in requirements language. Additionally, the SDT added the language to R2.3 "…for external routable protocol connections and Dial-up Connectivity" to address the support given in FERC Order 761, paragraph 87, for electronic security perimeter protections "of some form" to be applied to all BES Cyber Systems, regardless of impact.

Reliability Benefit and Double Jeopardy Concerns of Requirements R3, R5, and R6

Numerous commenters also raised questions about either the reliability benefit or double jeopardy of requirements R3, R5, and R6. Often, these questions were tied to work going on in NERC standards related to Paragraph 81 of the FERC Order approving the FFT process. The comments about their reliability benefit sometimes hinged on them being a requirement in and of themselves, rather than a component of the requirements for R1, R2, and R4 in draft two. The double jeopardy concerns also raised similar questions as to whether a violation of R3, R5, and R6 in draft two would also constitute a violation of R1, R2, and R4 of draft two. The SDT agreed with these concerns. The SDT believes that the same reliability and security objectives will be reached, while alleviating unnecessary compliance concerns, by combining these requirements. As such, the review and approval for each of the cyber security policies has been added as an obligation in the security policy requirements (R1 and R2) themselves. Additionally, the obligation to keep the CIP Senior Manager and delegation documentation up-to-date has been added to those requirements (now R3 and R4), respectively.

Modify Signature to Approval in Measures

Several commenters mentioned the use of "signature" in the measures when the requirement called for "approval." The SDT had never intended to imply that a wet ink signature was the only acceptable form of evidence of approval. Language in the guidelines and technical basis section further clarified that hardcopy or electronic approvals were acceptable. The SDT has modified all instances of "signature" in the measures in CIP-003-5 to "approval' to prevent any confusion and better align with the language in the requirement itself.

Minority Comments

The SDT also received a number of different comments that asked various questions or raised assorted concerns about the topics that were included in Requirement R1. Among other things, these comments mentioned confusion about the guidance related to terms used in the policy topics, inclusion of Interactive Remote Access separate from ESPs, and the relationship between these topics and CIP-004-5 through CIP-011-1. The intention of the SDT was for these policy items

to individually reference each of the standards CIP-004-5 through CIP-011-1. As such, the SDT has chosen to align the policy topics with the title of the other CIP standards (with some exceptions) and include a specific reference to the standards itself in order to clarify that alignment. As mentioned in the discussion of policy implementation above, the SDT's expectation is that implementation of the cyber security policy for medium and high impact BES Cyber Systems will be demonstrated through compliance with CIP-004-5 through CIP-011-1.

Typographical Errors

Several commenters also noted a typographical error where the VRF for CIP-003-5 R2 was listed as low in the requirement and medium in the VSL table. The SDT appreciates commenters pointing this out. The intention of the SDT was for the VRF of CIP-003-5 R1 for medium and high impact BES Cyber Systems to be medium, consistent with CIP-003-4 R1 and for the VRF of CIP-003-5 R2 to be low due to the lesser risk associated with low impact BES Cyber Systems. The SDT has corrected this mistake.

VSL Comments not responded to:

One comment suggested that Requirement R6 should have four VSLs based on days late. The SDT has removed the requirement because the addition of language to identify, assess, and correct deficiencies in what is now Requirement R4 covers the documentation of delegations.

One comment stated to start missing discrete elements of a program as low VSLs in Requirement R2. The SDT has made this change.

One comment suggested to use Lower/Moderate VSLs for Requirement R2 instead. In response, the VSLs only address the degree to which entities can violate a requirement and not the risk power to the BES from said violations.

For the Requirement R4 VSLs, there was a comment that the VSL should read: Lower/Medium – Lack of Review High/Severe – Lack of Approval. This requirement has been removed because the annual review is already accomplished in Requirement R1 and the need to have a CIP Senior Manager sign the policy is administrative in nature.

There was a comment that the VSL for Requirement R3 is more detailed than the requirement itself. The SDT has updated the VSL to match the requirement.

Questions with Votes Only:

1. **Requirement R1 of draft CIP-002-5 requires the identification of high and medium impact BES Cyber Systems as described in Attachment 1. Further, it requires a Responsible Entity to review (and update as needed), the required identification within 60 calendar days of when a change to BES Elements or Facilities is placed into operation, which is planned to be in service for more than 6 calendar months and causes a change in the identification or categorization of the BES Cyber Systems from a lower to a higher impact category. Do you agree with the proposed Requirement R1?**

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
BC Hydro	No
IRC Standards Review Committee	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No

Organization	Yes or No
Duke Energy	No
Dominion	No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	No
MRO NSRF	No
Florida Municipal Power Agency	No
Madison Gas and Electric Company	No
Luminant	No
SMUD & BANC	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
Western Electricity Coordinating Council	No
CenterPoint Energy	No
Tri-State G&T - Transmission	No
PacifiCorp	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Western Area Power Administration	No
Utility Services Inc.	No
Consumers Energy Company	No
Muscatine Power and Water	No
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	No
NIPSCO	No
Portland General Electric	No
TransAlta Centralia Generation LLC	No
Trans Bay Cable	No
National Grid	No
Hydro-Quebec TransEnergie	No
LCEC	No

Organization	Yes or No
Pacific Gas and Electric Company	No
Ingleside Cogeneration LP	No
Manitoba Hydro	No
Niagara Mohawk (dba National Grid)	No
PSEG	No
Bonneville Power Administration	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
Wisconsin Electric Power Company	No
The Empire District Electric Company	No

Organization	Yes or No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
Nebraska Public Power District	No
City of Austin dba Austin Energy	No
ISO New England	No
Network & Security Technologies, Inc.	No
City Utilities of Springfield, MO	No
American Public Power Association	No
Alliant Energy	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No

Organization	Yes or No
Indiana Municipal Power Agency	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Puget Sound Energy, Inc.	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Tennessee Valley Authority	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
PJM Interconnection	Yes
Kansas City Power & Light	Yes
MEAG Power	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes

2. Requirement R2 of draft CIP-002-5 states, "The Responsible Entity shall have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once each calendar year, not to exceed 15 calendar months between approvals, even if it has no identified items in Requirement R1, Parts 1.1, 1.2, or 1.3." Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
ACES Power Marketing	No
BC Hydro	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
SMUD & BANC	No
Progress Energy	No
PacifiCorp	No
Utility Services Inc.	No

Organization	Yes or No
NIPSCO	No
LCEC	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
ISO New England	No

Organization	Yes or No
Kansas City Power & Light	No
Indiana Municipal Power Agency	No
Brazos Electric Power Cooperative	No
PPL Corporation NERC Registered Affiliates	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Luminant	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency	Yes
Portland General Electric	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Flathead Electric Co-op	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Ameren	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
PJM Interconnection	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

4. CIP-003-5 R1 states "Each Responsible Entity for its high impact and medium impact BES Cyber Systems shall implement one or more documented cyber security policies that address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Duke Energy	No
Progress Energy	No
NCEMC	No
PNM Resources	No
AEP Standards based SME list	No
Xcel Energy	No
MidAmerican Energy Company	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Kansas City Power & Light	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Southwest Power Pool Regional Entity	Yes
NRG Companies	Yes
PNGC Comment Group	Yes

Organization	Yes or No
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Florida Municipal Power Agency	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
New York Power Authority	Yes
Tampa Electric Company	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
American Public Power Association	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

5. CIP-003-5 R2 states "Each Responsible Entity for its BES Cyber Systems not identified as high impact or medium impact shall implement one or more documented cyber security policies to address the following topics:" and then defines the areas that must be addressed in the policies. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
MRO NSRF	No
Florida Municipal Power Agency	No

Organization	Yes or No
Madison Gas and Electric Company	No
Pepco Holdings Inc & Affiliates	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
NCEMC	No
Dairyland Power Cooperative	No
AEP Standards based SME list	No
Snohomish County PUD	No
Edison Mission Marketing & Trading	No
Consumers Energy Company	No
Muscatine Power and Water	No
Lower Colorado River Authority	No
LCEC	No

Organization	Yes or No
LCRA Transmission Services Corporation	No
Ingleside Cogeneration LP	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service	No

Organization	Yes or No
Corporation and Upper Pennisula Power Company	
Nebraska Public Power District	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
MEAG Power	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes
BC Hydro	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Southern California Edison Company	Yes
SPP and specific Member companies	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
PNM Resources	Yes
Hydro One	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
NIPSCO	Yes
Portland General Electric	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
New York Power Authority	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
ISO New England	Yes
City Utilities of Springfield, MO	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
California ISO	Yes
US Bureau of Reclamation	Yes

6. CIP-003-5 R3 states "Each Responsible Entity shall identify a CIP Senior Manager by name." Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
ACES Power Marketing	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Southern Company Services, Inc.	No
Independent Electricity System Operator	No

Organization	Yes or No
Lakeland Electric	No
Tampa Electric Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
Texas Reliability Entity	No
City of Austin dba Austin Energy	No
Kansas City Power & Light	No
Network & Security Technologies, Inc.	No
American Public Power Association	No

Organization	Yes or No
Tucson Electric Power	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes

Organization	Yes or No
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
City of Palo Alto	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Xcel Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
New York Power Authority	Yes
Tennessee Valley Authority	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
ISO New England	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

7. **CIP-003-5 R4 states "Each Responsible Entity shall review and obtain CIP Senior Manager approval for cyber security policies identified in Requirements R1 and R2, at least once each calendar year, not to exceed 15 calendar months between reviews and between approvals." Do you agree with the proposed Requirement R4?**

Summary Consideration:

Organization	Yes or No
NESCOR/NESCO	No
ACES Power Marketing	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
Progress Energy	No
Edison Mission Marketing & Trading	No
Independent Electricity System Operator	No

Organization	Yes or No
Pattern	No
United Illuminating Company	No
Lakeland Electric	No
Tampa Electric Company	No
Tennessee Valley Authority	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
NYISO	No
Cowlitz County PUD	No
Brazos Electric Power Cooperative	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Texas RE NERC Standards Review Subcommittee	Yes
NRG Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
Western Electricity Coordinating Council	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes

Organization	Yes or No
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
New York Power Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Oncor Electric Delivery Company LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
City of Austin dba Austin Energy	Yes
ISO New England	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Tucson Electric Power	Yes
US Bureau of Reclamation	Yes

8. CIP-003-5 R5 states "Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate and the date of the delegation, and approved by the CIP Senior Manager." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
Southwest Power Pool Regional Entity	No
NRG Companies	No
Duke Energy	No
Florida Municipal Power Agency	No
Progress Energy	No
Hydro One	No

Organization	Yes or No
Independent Electricity System Operator	No
Xcel Energy	No
Flathead Electric Co-op	No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Wisconsin Electric Power Company	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper	No

Organization	Yes or No
Pennisula Power Company	
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
American Public Power Association	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes

Organization	Yes or No
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes

Organization	Yes or No
NIPSCO	Yes
Portland General Electric	Yes
Trans Bay Cable	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes

Organization	Yes or No
United Illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Kansas City Power & Light	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield,	Yes

Organization	Yes or No
MO	
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

9. CIP-003-5 R6 states "Each Responsible Entity shall document any changes to the CIP Senior Manager or any delegations within thirty calendar days of the change. Delegation changes do not need to be reinstated with a change to the delegator." Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Texas RE NERC Standards Review Subcommittee	No
NRG Companies	No
Florida Municipal Power Agency	No
Progress Energy	No
Portland General Electric	No
Independent Electricity System Operator	No
Flathead Electric Co-op	No

Organization	Yes or No
Lakeland Electric	No
New York Power Authority	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Public Service Corporation and Upper Pennisula Power Company	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
ISO New England	No
Kansas City Power & Light	No

Organization	Yes or No
American Public Power Association	No
Tucson Electric Power	No
Cowlitz County PUD	No
California ISO	No
ACES Power Marketing	Yes
PPL Corporation NERC Registered Affiliates	Yes
BC Hydro	Yes
IRC Standards Review Committee	Yes
Southwest Power Pool Regional Entity	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Dominion	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (JRO00088, NCR01177)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
MRO NSRF	Yes
Madison Gas and Electric Company	Yes
Pepco Holdings Inc & Affiliates	Yes
Southern California Edison Company	Yes
NCEMC	Yes
SPP and specific Member companies	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes

Organization	Yes or No
Hydro One	Yes
AEP Standards based SME list	Yes
Snohomish County PUD	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Edison Mission Marketing & Trading	Yes
Utility Services Inc.	Yes
Consumers Energy Company	Yes
Muscatine Power and Water	Yes
NIPSCO	Yes
Trans Bay Cable	Yes

Organization	Yes or No
Pattern	Yes
National Grid	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
LCEC	Yes
Pacific Gas and Electric Company	Yes
LCRA Transmission Services Corporation	Yes
Ingleside Cogeneration LP	Yes
Manitoba Hydro	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
PSEG	Yes
United Illuminating Company	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Xcel Energy	Yes
Bonneville Power Administration	Yes
Tennessee Valley Authority	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
NV Energy	Yes
Wisconsin Electric Power Company	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Network & Security Technologies, Inc.	Yes
City Utilities of Springfield, MO	Yes

Organization	Yes or No
MEAG Power	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Colorado Springs Utilities	Yes
Central Lincoln	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards

Comment Form B

CIP-004 through CIP-007 Questions

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 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.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
7.	Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8.	Annie Terracciano	Northern Lights Inc.	WECC 3										
9.	Aleka Scott	PNGC	WECC 4										
10.	Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12.	Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13.	Margaret Ryan	PNGC	WECC 8										
12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14.	Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	M & A Electric Power Cooperative	SERC	1, 3	
4.	Northeast Missouri Electric Power Cooperative	SERC	1, 3	
5.	N.W. Electric Power Cooperative, Inc.	SERC	1, 3	
6.	Sho-Me Power Electric Cooperative	SERC	1, 3	

15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Oglethorpe Power Corporation		SERC	5
2.	Georgia Transmission Corporation		SERC	1

16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWERENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
8.	SCOTT NICKELS	RPU	MRO	4
9.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
10.	MARIE KNOX	MISO	MRO	2
11.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
12.	SCOTT BOS	MPW	MRO	6, 1, 3, 5
13.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
14.	THERESA ALLARD	MPC	MRO	1, 3, 5, 6

17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	James Howard	Lakeland Electric	FRCC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Darl Shimko	MGE	MRO	3
2.	Joseph DePoorter	MGE	MRO	4
3.	Steve Schultz	MGE	MRO	5
4.	Jeff Keebler	MGE	MRO	6

20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Jones	Pepco	RFC	1

21.	Group	Rick Terrill	Luminant					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6
9.	Brenda Hampton	Luminant Energy Company LLC		

22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Smith	BANC	WECC	1

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				

Additional Member	Additional Organization	Region	Segment Selection
1. Rayburn Country Electric Cooperative		SPP	
2. Empire District Electric		SPP	1
3. City Utilities of Springfield		SPP	4
4. Westar Energy		SPP	1, 3, 5, 6
5. Cleco Power		SPP	1, 3, 5, 6

25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						

Additional Member	Additional Organization	Region	Segment Selection
1. Pawel Krupa		WECC	1
2. Dana Wheelock		WECC	3
3. Hao Li		WECC	4

27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					

Additional Member	Additional Organization	Region	Segment Selection
1. Denise Lietz	Puget Sound Energy	WECC	1
2. Erin Apperson	Puget Sound Energy	WECC	3

28.	Group	Michael Mertz	PNM Resources	X		X							

Additional Member	Additional Organization	Region	Segment Selection
1. Laurie Williams	Public Service Co. of New Mexico	WECC	1
2. Michael Mertz	Public Service Co. of New Mexico	WECC	3

29.	Group	Sasa Maljukan	Hydro One	X									

Additional Member	Additional Organization	Region	Segment Selection
1. David Kiguel	Hydro One	NPCC	1

30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION B8 – CIP-004-5, R1, R2, R3, R4 or R5:

If you disagree with the changes made to CIP-004-5, Requirements R1, R2, R3, R4 or R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, the SDT made significant changes to the requirements, measures, and VSLs associated with Requirement R1, R2 R3, R4 or R5 of CIP-004-5. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity.

Note
In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5. For the purposes of the comment summaries and responses for this question, the requirement number references refer to the requirement numbers as listed in draft 2, unless otherwise noted.

General
The applicable systems section has been reviewed and revised to help ensure consistency within CIP-004-5 and with the other CIP standards. This should also make clear that these requirements are not applicable to Low Impact BES Cyber Systems. The SDT has decided not to include the concept of authorized unescorted electronic access. Individuals with

authorized electronic access must be trained and have a personnel risk assessment performed as per the requirements. This applies to all personnel including employees, vendors and contractors. For example, the question on a vendor controlled system would require the vendor to meet the requirements as set forth in CIP-004-5.

The SDT has stricken the "attain and retain" language for the training requirement, but has chosen to keep it for the personnel risk assessment requirements. The difference between those words and "acquire and maintain" are negligible.

The SDT does not agree with the suggestion to make Requirements R2 and R3 an expansion of the awareness program instead of training. The SDT believes that for protection of these BES Cyber Systems more targeted training is needed.

The guidelines and technical basis section has been updated to better align with the new draft content and organization. One areas of focus is the training content on networking hardware and software and other issues of electronic interconnectivity. More description around the criminal history check has also been added.

Requirement R1

The SDT has added language in the change rationale section to reinforce the concept that a registered entity does not need to ensure or prove all authorized personnel have received awareness. The language in R1.1 has also been revised to further clarify this point through the use of the word, reinforces. Also, the SDT has added language to clarify that awareness of cyber security practices can include physical security information.

The SDT appreciates the suggestions to allow the registered entity to define the timeline for awareness reinforcement or their own quarters, but believes the language is best retained as written for consistency.

In the measures for Requirement R1, the SDT has removed the reference to "documented security awareness program" and has modified the language to be consistent with the other CIP standards. The language, "not limited to" has also been revised and reviewed for consistency across the standards.

Requirement R2/Requirement R3

These two requirements have been combined into a single requirement which covers the training content in R2.1, in a single table, and the training frequency in R2.2 and R2.3. Another key change in R2 is the modification of the language to clarify that the registered entity is able to determine their training program(s) to fit their needs and it can be based on role, function or responsibility. In concert with this change, Table R2 section 2.1 was deleted to help eliminate the

language focusing on role based training. Training is required of individuals with authorized, unescorted physical access or authorized electronic access as per the revised R2.2 and R2.3. In addition to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity, the SDT believes training is also needed for individuals with access to Physical Access Control Systems and Electronic Access Control or Monitoring Systems. Also, the SDT has removed the reference to BES Cyber Systems in Table R2 formerly in sections R2.2, R2.3 and R2.4. For Table R2 previous section 2.5, the Change Rationale has been modified to reflect this is a new training requirement. Also, this training should be tracked for personnel involved in the visitor control process in accordance with Table R3 section 3.2 The SDT agrees that recovery plan information referenced in Table R2, previous section 2.8 should be labeled appropriately. The training content on cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets will remain in Table R2 as it is a new requirement from FERC Order 706 and the SDT has provided additional guidance to clarify the intent of this entry.

For Table R2, previous section 2.2, the SDT believes the training should be focused on policy content, not availability, and has made no changes. In Table R2, the SDT has chosen to retain both identification of incidents and response to incidents as separate content as the personnel who need to be trained on each may be different. The scope of training on recovery plans is left to the registered entity and no changes have been made to the standard. Also, the SDT believes the focus of recovery is the specific recovery plans, not the business impact analysis. The measure for Table R2 has been modified to focus on training material as evidence and the guidance has been revised to reflect the type of content this training should include.

The SDT has edited the language formerly in R3 for clarity with removal of the role based reference and the attain/retain language. Since there are no references to evidence retention in the requirement part 1.2, evidence retention, of the compliance section of the standard applies. The reference to documentation that was in Table R3 section 3.1 has been removed as it is covered in the measure.

The SDT does not agree that access to Low Impact Cyber Systems need the training defined in R2. Also, R2 has language included (in a manner that identifies, assesses, and corrects deficiencies) as suggested by some comments to allow detection and correction of flaws. The proposal to allow the registered entity to define the timeline for training was not supported by the SDT. For 2.2 and 2.3 (formerly in Table R3 section 3.2), the SDT believes the language is sufficiently clear that the time interval is between training dates and does not need that language added. BES Cyber Systems was changed to applicable cyber assets in 2.2. The two entries on initial and recurring training are now in Table R2. The SDT

has revised the language in the measure for these two entries to make it clear the focus is on training records which should include training date and date access is granted.

Requirement R4/Requirement R5

As suggested, the SDT has combined these two requirements into one and it is now Requirement R3. The SDT has modified the language formerly in Requirement R4 to help clarify that identity confirmation and criminal history check are part of the personnel risk assessment (PRA). The PRA is the outcome of the process or criteria used by a registered entity to evaluate the results of the identity verification (for the initial PRA) and seven year criminal history records check to determine what, if any, authorized access to grant to employees, contractors or vendors. The level of documentation for the process or criteria is left to the registered entity, but should be sufficient for a third party to understand how the decision is made. In defining the seven year criminal history records check, it is not the intent for the registered entity to evaluate the individual's residence locations, education or prior employment. The language has been revised to indicate the criminal history records check should cover locations where the individual has resided/lived for six consecutive months during the past seven years. The initial identity confirmation, even if performed under prior versions of the standards, is sufficient for the employment duration of the individual. The initial identity verification, criminal history check and PRA should be retained in accordance with requirement part 1.2 in the evidence retention component of the compliance section of the standard. A PRA performed under previous versions of the standards is valid until it reaches the end of its seven year lifespan. The intent of the SDT is that the PRA in effect is no older than seven years. The SDT has provided guidance on the acceptable documentation for an exception to the seven year criminal history records check which includes agreements with labor unions. If the registered entity is unable to fully complete the seven year criminal history records check, the SDT feels it is important to document the reasons for the exception so it will not be removing that piece of the requirement. Also, the timeframe for renewal of the criminal history records check is currently seven years and the SDT believes it should remain as such. Drug and alcohol checks are typically performed by entities under an existing program and the SDT chooses not to add this to the requirement. In section 3.3 of the new Table R3, the term process is used to define the method used by a registered entity to evaluate the results of the criminal history records check. Although a "Transportation Worker Identification Credential (TWIC)-like" program would be helpful to facilitate compliance with the PRA requirements, the SDT does not have the authority to make that happen. Measures – The Measures have been revised to focus on examples consisting of documentation. For example, a dated copy of the current PRA, which was performed in the previous seven calendar years, would be sufficient.

VRF/VSL

The language in the VRF for R2 has been changed to remove the reference to role based training. The SDT reviewed the VRFs for R3, R4 and R5 (as indicated above, R3 from draft 2 is now in R2, and R4 and R5 from draft 2 have been combined into R3 in draft 3) to consider if the rating should be a Lower risk factor. The SDT believes the risk associated with violations of these requirements is higher than for R1 and R2; hence the Medium risk factor is appropriate. The VSL for R1 has been modified to include the case where the Responsible Entity failed to implement on-going security awareness for two or more consecutive quarters as the next step above the criteria for High. Since the Medium severity level is for missing two content topics, the High should follow as three or more, not four or more. Commenters also asked whether the size of the company matters in the VSL for R3 (which is now in R2). In response, the SDT has modified the VSL for High and Severe according to the suggestion. The VSL targets the BES Cyber System and does not account for company size. Commenters suggested the Moderate and High VSL language for R4 (now R3) should be swapped on the basis that not performing an identity verification and a background check is worse than failing to document the results. (Also, the incorrect reference in draft 2's R4 to "4.5", which does not exist, has been corrected). In response, the SDT has modified the language for the Severe VSL to include the case where a registered entity failed to implement its PRA processes. Commenters also asked whether the size of the company matters in the VSL for R5 (which is now in R3). In response, the VSL targets the BES Cyber System and does not account for company size.

QUESTION B9 – CIP-004-5, R6 or R7:

If you disagree with the changes made to CIP-004-5, Requirements R6 or R7 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the major concerns with CIP-004 Requirements R6 and R7 center on removal of access privileges under various categories of termination actions. In addition, there were repeated instances noting a lack of clarity regarding access approvals, personnel transfers or reassignments and the proper storage and handling of NERC CIP information.

Note

In draft two, Requirement R2 required a documented process for its role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems while Requirement R3 was the implementation of that process. Requirement R4 required one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems while Requirement R5 was the implemented of the one or more documented processes. In preparing CIP-004-5 for draft 3, the SDT determined that Requirements R2 and R3 could be combined, and so could Requirements R4 and R5. In that way, the requirements more closely match most other requirements in CIP-004-5 through CIP-011-5 to implement a documented process, and it also facilitated inclusion of the correcting deficiencies approach, explained in the common response section of this comment response, so that the resulting requirements, draft 3's Requirements R2 and R3, could be implemented "in a manner that identifies, assesses, and corrects deficiencies." Therefore, Requirement R6 from draft 2 was renumbered to Requirement R4 in draft 3, and Requirement R7 from draft 2 was renumbered as Requirement R5.

Applicability Section

As in other Version 5 standards, in CIP-004, requirement part 4.1 (formerly part 6.1), there were several comments on changing instances of Medium Impact BES Cyber Systems to "Medium Impact BES Cyber Systems with External Routable Connectivity." Commenters also commented that "dial-up connectivity" should be removed from the applicability section to be consistent with the applicability sections of other Version 5 standards. In both of these cases, the SDT has revised the standard to reflect these comments.

Requirement R4 (formerly R6) General Comments

Multiple commenters recommended that new or additional items or items currently found in the rationale section should be modified and listed as requirements at the requirement level.

Comments suggested modification to allow for self-correction in certain cases, so that each responsible entity shall implement: measure performance to detect flaws; correct detected flaws expeditiously, and if needed take corrective action to prevent recurrence of flaws. This is a general requirement that applies to the Requirement R4 (formerly R6) sub requirements. Though not necessary from a procedural perspective, more instruction on what needs to be considered in the standards is better than insufficient information. The SDT has incorporated the correcting deficiencies modification to the implementation wording in CIP-004-5 in Requirements R2, R3 and R4.

Commenters recommended that the rationale discussing controls for BES Cyber Systems without user accounts should be added to the appropriate requirements in Requirement R4 (formerly R6). The SDT has moved that discussion from the rationale section to the requirement tables.

A commenter suggested that requirement parts 4.2, and 4.3 (formerly covered in parts 6.2, 6.3 and 6.4) be modified to include requirement parts 4.11, 4.12 and 4.13 (formerly parts 6.11, 6.12 and 6.13) along with part 4.1 (formerly part 6.1) in the requirement table. The SDT has combined requirement parts 4.2, 4.3 and 4.4, which now directly reference those sub-parts in part 4.1.

R4.3 (formerly 6.3)
Commenters recommended that there be a corresponding annual review of provisioned physical security privileges necessary for performing assigned work functions. The SDT has combined requirement parts 4.2, 4.3 and 4.4 (formerly parts 6.2, 6.3 and 6.4). The measures in the new requirement part 4.2 call for signed documents, automated workflow approvals or email showing persons with access have authorizations and similar or the same records showing the consideration of appropriate privileges on the basis of need…" These measures apply to electronic access, unescorted physical access into a PSP and access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Part 4.3 (formerly part 6.5)
Commenters asked for clarification on the reviews of authorized and provisioned electronic access and unescorted physical access. The SDT has modified part 4.3 to clarify the requirement. It now reads "verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records."

R4 (formerly R6)

Some commented that the measures for 4.1 (formerly part 6.1) should include unescorted electronic access. The issue with this is that electronic access, by its digital nature cannot be escorted. Consequently, there is no "unescorted" electronic access. Electronic access to data or systems is either authorized or unauthorized. One could call it "supervised" access but the problem lies with a "supervisor" having to be continuously diligent and unerringly able to determine if the supervised user is doing anything malicious. This is not possible and frankly constitutes a threat to network integrity and data confidentiality. The recommended option would be to identify those contractors who require electronic access and run them through the personnel appraisal and the training processes and grant them appropriate access privileges. There are no other means to help ensure there are no unauthorized accesses or data disclosures.

Requirement Part 4.1 (formerly 6.1)

One commented that formerly sub-requirements 6.1.1, 6.1.2 and 6.1.3 (current 4.1.1, 4.1.2 and 4.1.3) would be clearer if the requirement was written, "Designate one or more individual(s) to authorize one or more of the following types of access". The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter suggested that current requirement part 4.1 should include the names and roles of individuals who authorize the various types of access. The SDT has changed the requirement to "have a process to authorize". This negates the need to specifically identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information.

One commenter recommended changing the term "designate" in current requirement parts 4.1, 4.2 and 4.3 (formerly parts 6.1, 6.2 and 6.3) to "identify.' The SDT has changed requirement 4.1 to "have a process to authorize". This negates the need to specifically designate or identify an approver and highlights consideration of "need" for physical access, electronic access and access to "designated" physical and electronic storage locations for BES Cyber System Information. The SDT has also combined 4.2, 4.3 and 4.4 into a single requirement (4.2).

Several commenters pointed out that access to physical and electronic locations where BES Cyber System Information is stored should have greater clarity around the word "physical". The requirement part 4.1 (formerly part 6.1) has been

changed to clarify storage locations for BES Cyber System Information. It now reads, "access to designated storage locations, whether physical or electronic, for BES Cyber System Information.

Several commenters recommended revising the phrase "unescorted physical access" to "unescorted physical access into a PSP." The SDT agrees and has made that change.

Multiple commenters stated that requirement part 4.1 (formerly part 6.1) should allow for roles in the designation of those individuals who can authorize the various accesses. The SDT believes that changing the requirement to "have a process" allows the entity the flexibility to construct their authorization process in a way that best suits their needs.

Requirement Part 4.2 (formerly Part 6.2)
Several commenters recommended that requirement parts 6.2 and 6.3 be revised for clarity. They proposed that requirement parts 6.2 and 6.3 be changed to read, "the individual(s) or role(s) designated in requirement part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." To respond to the comment, requirement parts 4.2, 4.3 and 4.4 have been combined into a single requirement part 4.2. At the same time, the individual authorization has been replaced with a process in requirement part 4.1. The process merely provides a means to authorize, and is implemented in the manner preferred by the Responsible Entity.

Several commenters also suggested that instead of the phrase "deemed necessary," "deemed appropriate" would be more accurate – stating that deeming appropriate is easier than deeming necessary. The SDT used the term "necessary…for performing assigned work functions" to better focus on specific accesses and minimize generalization and audit interpretation issues.

One commenter suggested the phrase "Responsible Entity" be removed from parts 4.2, 4.3 and 4.4 (formerly 6.2, 6.3, and 6.4). The requirements state "that the Responsible Entity determines is necessary." The SDT believes that the term "Responsible Entity" removes a degree of specificity that could be problematic if individuals change frequently or the determination of "necessary" is made by more than one individual within the organization. The SDT has combined requirement parts 4.2, 4.3 and 4.4 and has referenced a process required in part 4.1 "have a process" that allows flexibility to establish authorization frameworks tailored to the Responsible Entity's needs.

One commenter stated that the phrase "need to know" in requirement part 4.2 (formerly Part 6.2) is difficult to quantify and is subject to interpretation. They recommended removing that phrase, believing that approvers who grant all access

"deemed necessary" strongly indicates that determinations of need to know are part of the authorization process. The SDT has removed references referring to "need to know."

Many commenters recommended revising the phrase "unescorted physical access" to read "unescorted physical access into a PSP." For clarity, the SDT has changed the wording to "access into the Physical Security Perimeter."

One commenter stated that requirement part 6.3 (now covered under new part 4.1) implies that determination of need for performing work functions is needed for each physical access. They recommended that Responsible Entities document all roles and activities in advance, negating the need for the Responsible Entity restating access they have "determined is necessary." The SDT has combined the requirement parts 4.2, 4.3 and 4.4 and established a requirement for a "process" to develop an authorization framework best suited to the Responsible Entity's needs. This will allow the commenter's company to document all roles and activities in advance if that is the company's preference.

One commenter recommended removal of the phrase "for performing assigned work functions" due to concerns with potential interpretation requests. The SDT believes that since "work functions" are not subject to audits, there is no need to remove the conditional phrase. In addition, there must be some frame of reference for authorizing accesses and work functions are a logical baseline.

Many commenters suggested changing the wording of requirement part 6.4 (now covered under new part 4.1) from "location" to designated repository. The SDT believes that specifying a designated location is less subject to interpretation and in most cases exempts portable equipment from being identified as a "repository" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

One commenter questioned the following: Is the "intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format?" The SDT believes that unescorted physical access includes to both hard copy data and access to equipment used for storing electronic copies. Although physical proximity to equipment does not constitute electronic access, from

an information protection standpoint, access to that equipment could result in damage or destruction of those devices storing electronic copies.

One commenter suggested that in requirement part 6.4, (now covered under new part4.1)to eliminate ambiguity, that the term “necessary for performing assigned work functions,” be replaced with “appropriate for the roles and responsibilities.” The SDT understands the concern. In this case replacing “necessary” with “appropriate” does little to eliminate ambiguity. In addition, both terms are likely to prompt interpretations. Also, not all entities are configured to grant authorizations by roles and responsibilities. To address the entirety of the CIP affected population, the SDT believes that the original wording provides more universal applicability.

One commenter believes that requirement part 6.4 (now covered in new part 4.1) should be separated into two requirements. The first requirement would be to identify the repositories that store either physical media containing BES Cyber System Information (paper copy) or the electronic storage of BES Cyber System Information. The second requirement would be the authorization of access to only those designated repositories that have been identified by the entity. The SDT believes that using the term “locations”, as long as they are “designated” serves the same purpose as an identified repository. Because “designated” has been added to the requirement, so must a measure to acknowledge the existence and itemize “designated storage locations.” This will add another measure but will also reduce the potential for audit interpretation and ambiguity.

One commenter recommended that the words “are necessary for performing assigned work functions” be replaced simply with “are necessary”. The SDT believes that this revision, although more economical, could create a situation where the question is asked “necessary for what?” To avoid that possibility “necessary for assigned work functions” is less likely to prompt questions of scope of authorizations.

One commented that the words “physical and” should be removed because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. The SDT notes that if, as suggested by a number of other companies, “designated locations” are used, incidental, non-designated temporary locations of NERC CIP System Information will not be subject to that requirement.

Former Requirement Part 6.3

Former requirement part 6.3 prescribed specific ways to conduct authorizations and referenced individuals designated in former part 6.1. The SDT has instead changed the language in part 4.1 to require the Responsible Entity to "Have a process to authorize . . .", which could certainly include designating one or more individuals, etc., as part of the process, but the requirements do not specifically prescribe the administrative method of achieving the required performance. Thus, former Requirement Part 6.3 no longer exists in the same manner as presented during draft 2.

Several commenters stated that because of potential minor errors or mismatches associated with the required review of authorizations and provisioned individuals, requirement part 4.3 (formerly part 6.5) should be subject to the FFT process. The SDT understands the concern, but FFT is not a function of the requirement. That is a function of potential violations and determined after the fact, not in the standard requirement itself.

One commenter recommended that the following statement from the rationale for requirement part 4.3 (formerly part 6.5) be entered into the requirement or its Measures section: "If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement." While that statement offers some clarification in guidance, the SDT cannot add a requirement or measure that makes a determination whether or not a particular error is a violation.

One commenter stated that requirement parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) are major scope expansions which were not directed by FERC. They further claim that the requirements overlap and are not contributing to a commensurate improvement to security. The SDT believes that reviews such as those in parts 4.3 and 4.4 (formerly parts 6.5 and 6.6) do in fact provide a means to identify indicators of malicious activities, rogue accounts, retained accounts that are no longer authorized, etc. The fact that FERC did not direct the requirement development does not negate the validity or the need for the requirements.

Several commenters recommended adding "currently" between "individuals provisioned". The SDT agrees with the recommendation and will take appropriate action. The SDT has reworded the requirement part 4.3 (formerly part 6.5) to "individuals with an *active* electronic access…"

One commenter stated that requirement part 4.5 (formerly part 6.7) should be revised as follows, “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records.” The SDT believes that there must be a specified review period and associated evidence to ensure that Responsible Entities consistently meet the requirement.

One commenter suggested adding the words "to BES Cyber Systems" after the words "physical access" in part 4.3 (formerly part 6.5). The SDT believes this proposed revision is already addressed in the Applicable Systems section of the requirement.

One commenter suggested that in the measures section, there should be consistency of word order between "dated document of verification..." and "documentation of dated verification”. The first measure asks for “dated documentation of verification,” which simply provides a point in time wherein the verifications were performed. The second measure requires a document that provides times of specific verifications themselves, of authorization for access and provisioning of access. The SDT changed the language to provide clarity and consistency to the measure. The consistent language now reads, “dated documentation of the verification.”

Requirement Part 6.4

One commented that the measures in requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) contain contradictory constructions. The background section states that a numbered list includes all required evidence. In the measure, however, these parts state that evidence “may include, but is not limited to.” The SDT has added the phrase “that includes all of the following” to reconcile the format with the intent of the measure.

Several commenters stated that the wording in requirement part 4.4 (formerly part 6.6) is too prescriptive, specifically “verifications that all user accounts, user account groups, or user role categories and their specific associated privileges.” They proposed substituting that wording to read, “verifications that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities.” The SDT believes that the word appropriate is too vague and subject to interpretation. The goal is to verify access to specific accounts. In this case, the existing wording maintains the scope and leaves no ambiguity around which accounts require verification. Regarding the list of measures, the SDT has revised the measure by adding “that includes all of the following” to reconcile the format with the intent of the measures.

Several commenters stated that the measures should only require verification that the entity performed the verification while leaving the results of the verification out of the measure. The SDT believes that requiring verification should

specify those items to be verified. Asking for a "listing of all accounts/account groups", a "description of privileges", "accounts assigned" and 'verification that privileges are authorized and appropriate" does not expand scope. Confirming that "verification" was performed would assume that all registered entities would perform the verification on the same lists of required items. If the items are not articulated, there are no assurances that the data would be consistently derived or complete.

One commenter recommended changing the words "performing assigned work functions" to "are appropriate". The SDT believes that the use of appropriate to define specific standard provisions is too vague and subject to interpretation.

One commenter stated that the scope of requirement part 4.4 (formerly part 6.6) has been expanded above and beyond what has been directed by FERC. The SDT has taken very positive steps to meet the requirements of the FERC directives. In establishing some requirements, the only way to effectively validate that the provisions have been met is to identify the need for specific information that links the requirement to the compliance actions. There may be an increased number of these instances. The important factor is that FERC directives do not limit the detail of the required evidence. The SDT believes that the requirement and measures increase the level of security. Unauthorized, expired or mis-assigned access to BES Cyber Systems represents potential vulnerabilities that could be exploited if not addressed with these administrative requirements.

One commenter also recommended that the wording of the "annual requirement" be worded as follows, "once each calendar year of a period not to exceed 15 calendar months between verifications." The SDT has changed the requirement to read "once every 15 calendar months to incorporate the additional 3 months of previously discretionary time directly into the requirement."

One commenter believed that the word "all", referring to user accounts is too broad. Dominion suggested that the word "applicable" be added after "all" to point to those user accounts, etc that are directly associated with the requirement. The SDT has changed the requirement to read "user accounts on all applicable cyber assets" to maintain the appropriate scope of the requirement.

One commented that requirement parts 6.6 and 6.7 should be revised to allow responsible entities to perform verifications of user accounts, user account groups or user role categories and their specific associated privileges at "a timeframe that the Responsible Entity deems necessary." NextEra also suggested that this also applies to verifying "access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity

are correct…" Although there are a number of companies that would comply with the requirement according to its intent under a self-imposed timeframe, there is no way to ensure that this would be the case. The SDT feels that the annual requirement should remain in place to help ensure consistent compliance actions.

Several commenters recommended changing requirement parts 6.6 and 6.7 to remove "all" referring to reviews of user accounts, user account groups, or user role categories. They recommend replacing "all" with "BES Cyber Systems." The SDT believes that reviews should be performed only on applicable cyber assets. The requirement has been revised as follows: "that user accounts on all applicable cyber assets, user account groups, etc.

Some commenters also commented that "locations" in requirement parts 6.4 and 6.7 should be replaced with designated repositories and include a requirement to list the repositories. The SDT has reworded the requirement to read "designated storage locations for BES Cyber System Information, whether physical or electronic." It has also added a requirement to designate storage locations and a measure to provide a list of designated storage locations. This will remove incidental temporary storage on non-designated devices from the audit process.

Some commenters suggested that the language in the second measure, "A summary description of privileges associated with each group or role", be removed. The SDT believes that understanding the privileges associated with specific roles is a necessary data point for verification that the privileges for specific groups are authorized and appropriate for the work functions performed by those assigned to the groups.

Requirement Part 6.5

Many commenters suggested in some manner to move former parts 6.1, 6.4, 6.7, and 7.3 (now, collectively, parts 4.1, 4.5, and 5.3) into CIP-011. In response, the SDT has revised former parts 6.1 and 6.4 to require a process without specifying how to conduct the authorizations. The SDT notes that CIP-004-5's authorization requirements relate to individuals' access, while CIP-011-1 specifies the information protection requirements.

Some commenters expressed concerns that the measures of requirement part 4.5 (formerly part 6.7) do not need to include the phrase "the minimum necessary for performing assigned work functions." In response, one of the most important aspects of authorizations and privileges is that they be granted using a "least privilege" approach. Otherwise the possibility exists that authorizations are provided or maintained for individuals who do not need them based on expediency rather than a comprehensive review.

One commenter suggested removing the term “minimum” from the third measure of Part 4.5 (formerly part 6.7) since it was removed from the requirement. The SDT agrees with this suggestion and has revised the measure accordingly.

One commenter recommended that the word “privileges” be added to part 4.5 (formerly Part 6.7) after the word “access.” The proposed wording of the requirement would be “verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." The SDT concurs with this addition since it adds clarity to the requirement. It has added “privileges” to the requirement. In a related recommendation, another commenter suggested the word “privileges” be removed from the measure since it is not in the Part 4.5. Adding the word privileges as discussed above will alleviate those concerns.

Some commenters recommended removing requirement parts 4.4 and 4.5 (formerly parts 6.6 and 6.7) because they are too prescriptive in their attempt to accomplish requirement part 4.3 (formerly part 6.5). The SDT believes that verification of requirement part 4.3 hinges upon the existence and validation of requirements listed in 4.4 and 4.5.

One commenter also questioned whether a listing of authorizations is the same as a list of those with access. Authorizations provide a type of eligibility for access. A list of those with access may include someone without that authorization and a potential security issue. That is why the reviews of authorizations, access and privileges are critical to compliance with the standards requirements.

Requirement R5 (Formerly R7) Applicability Section

A few commenters suggested that the applicability of revocation requirements in CIP-004-5 R5 (formerly R7) for interactive remote access should be modified to exclude dial-up connectivity. In response, the dial-up connectivity reference is removed from CIP-004-5 in its entirety.

Commenters also recommended that applicability to “Medium Impact BES Cyber Systems” be limited to those with “External Routable Connectivity” to maintain consistence with other cyber systems/assets currently covered by similar requirements in CIP-004. External Routable Connectivity has already been added to the applicability section for CIP-004.

Requirement R5 (Formerly R7) General Comments

Several commenters expressed concern on requirement part 5.2 (formerly part 7.2) for transfers and reassignments. They believe that the timing of access removal should be based on the determination of when access is no longer necessary, rather than limiting it to a specific time frame related to the transfer or reassignment date. The SDT has revised part 5.2 (formerly part 7.2 as follows: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access".

For requirement part 5.1 (formerly part 7.1), a commenter suggested that part of the FERC Order 706 be more clearly reflected in the requirements. Specifically they would like documentation in the requirement that highlights FERC's statement that exceptions to revocation policy are allowed as long as they are properly documented for audit purposes. Paragraph 462 of Order 706 states that, "revocation should be immediate upon the employee's notification of any personnel action requiring revocation of access. However, the ERO may define what circumstances justify an exception that is other than immediate and determine what is the fastest revocation possible." In response, this is not a SDT issue. Creating exceptions for directives in a FERC Order is a separate process undertaken by the ERO. In any event, it is not simply a documentation requirement. Circumstances warranting exceptions have to be identified and then approved. This of course is done against a backdrop of "immediate" revocation stated in the order.

A few recommended that the requirement for revocation based on the "next calendar day" should be changed to "next business day." Another commenter proposed that "next calendar day" be replaced by "within 24 hours." The SDT believes that next business day does not fall under the intent of the FERC Order Directives. Next business day if a weekend or holiday period is in progress could extend the revocation process for two or three additional days. "Within 24 hours" is actually less time than is allowed by the "end of the next calendar day." For the purposes of these comment responses, the SDT feels that next calendar day best meets the FERC Order directive and provides better security than next business day.

Some commenters also expressed concern that the 24 hour revocation requirements may not realistic given numerous and diverse HR and IT processes throughout the industry. Essentially they, along with one other commenter, advocated returning to a framework that allows different time frames for different types of termination actions. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating

a process (which may allow for internal processes that serve as trigger points) at the time of the termination action and completing the process within 24 hours, the SDT believes this is a reasonable time frame.

Requirement Part 5.1 (formerly 7.1)
Commenters recommended that the criteria for termination action timeframes should include a reference to the communication of the intention to terminate to provide a type of time stamp for gauging compliance with related requirements of the standard. While the communication of a termination action is not mentioned specifically in the requirement, initiating the process required by requirement part 5.1 (formerly part 7.1) would probably include those trigger points for individual companies. This allows greater flexibility and more concise monitoring of the required timeframe.

Several commenters expressed concern with the format of the measures in Requirements R4 and R5 (formerly Requirements R6 and R7). They are concerned that the background section states that all numbered lists in the measures are all required evidence. However, the measure list states that the "evidence may include but is not limited to." The SDT has revised the measures by adding the following statement: "An example of evidence may include, but is not limited to *documentation of all of the following*: This sentence is followed by numbered measures. This is primarily a formatting issue and this revision should alleviate the discrepancy.

One commenter suggested that the requirement should include "disable or revoke all individualized domain user accounts held by the terminated staff." The SDT believes that removing unescorted physical (preventing any entry into an entity's facilities) and interactive remote access should prevent any further access by the individual after termination.

Some commenters stated that requiring access revocation within 24 hours for all types of terminations is overly burdensome. They believe the 24 hour requirement should be limited to "for cause" terminations with additional flexibility built in for other situations. Other commenters recommended that the 24 hour time frame should apply only to High Impact Assets. The SDT has revised the requirement to state that there must be a process to initiate removal of an individual's ability for unescorted physical access and interactive remote access. This is based on the premise that removal of the ability for access may be different than deletion, disabling, revocation or removal of all access rights. Considering that what is required is initiating a process (allowing for internal processes) at the time of the termination action and completing the process within 24 hours, the SDT feels this is a reasonable time frame.

A few commenters stated that requirement parts 5.1 and 5.5 (formerly parts 7.1 and 7.5) seem inconsistent regarding shared user accounts. The SDT sees no inconsistency and believes that the current requirements are clear and sufficiently differentiated. Requirement part 5.1 considers the first tier of access; unescorted physical and interactive remote electronic access. Requirement part 5.5 specifies changing passwords for shared accounts and provides a 30-day time frame for its completion.

One commenter recommended a change to part 5.1 formerly part 7.1) that changes the 24 hour requirement to the end of the next business day after the effective date and time of the termination action. The SDT believes this falls outside of the FERC Directive intent, particularly as it applies to the "next business day." The next business day could increase the access revocation time frame to well over the 24 hours currently stated in the requirement.

One commenter recommended that requirement parts 5.1 and 5.3 (formerly parts 7.1 and 7.3) be revised to include a statement on extenuating circumstances associated with the impact of completion of revocation within 24 hours. FERC has allowed "extenuating operating circumstances" which have a specific application in requirement part 5.5 (formerly part 7.5), due to the complexity and scope of the password change task. Extenuating circumstances outside of that definition are undefined and could be misconstrued as any circumstance that is perceived as an impediment to completion of the requirement. In addition, adding "extenuating circumstances" to these requirements could set a precedent for other requirements, negating the timeliness and effectiveness of underlying security intent.

One commenter suggested clarifying language to the wording of the requirement to make it clear that the 24-hour clock is related to the initiation of the termination process, not the complete termination actions themselves. The SDT has clarified that there must be a process to initiate removal of an individual's ability for access. Initiation of the process must be concurrent with a termination action. Completion of the removal is required within 24 hours of initiating the process.

One commenter believes that termination criteria should vary according to the situation. They would like the tightest timeframes reserved for terminations for cause. The SDT has maintained the 24 hour requirement for termination actions based mainly on the FERC 706 Order requirement that termination be executed immediately.

One commenter commented on a situation where a suspended individual is terminated ten days from the suspension date. While the termination action was initiated in compliance with the requirements of R5 (formerly R7), the effective date of the termination shows up in the records as 10 days prior to the action being initiated. The SDT believes that in

these situations, documentation of the suspension along with what a suspension entails regarding any network or system accesses, and a documented company statement verifying the entities suspension procedures and subsequent termination should be sufficient to provide evidence of compliance to an auditor.

Requirement Part 5.2 (formerly 7.2)
Many commenters are concerned about the 24 hour requirement for removal of access for those individuals transferred or reassigned. The SDT understands the issue with access often being required after the transfer for various lengths of time. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement to the following: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access."

One commenter would like reassignments or transfers based on the notification of reassignment or transfer. Rather than specify numbers of days within which an entity must complete the reassignment or transfer activities, the SDT has reworded the requirement and proposes the following changes: "For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

Requirement Part 5.3 (formerly 7.3)
A few commenters requested clarification on physical access to BES Cyber Systems and storage requirement wording in general. The requirement specifies that the access applies to those "designated physical and electronic locations where BES Cyber System Information is stored." In the requirement the term "designated" has been added. For the measures, evidence includes workflow or sign-off forms verifying access removal to "designated" physical areas or cyber systems. The term designated removes the unintended consequence of BES Cyber System Information temporarily resident on work stations, laptops, flash drives, etc. These areas are consequently not identified as storage "locations."

Some commenters suggested replacing the words "by the end of the next calendar day" to "within 7 days" or 30 days, respectively in the requirement. The SDT believes that since access removal in requirement part 5.1 (formerly part 7.1) will in many cases, constitute removal of access to BES Cyber System Information, that this requirement should retain its

original wording. In addition, in FERC Order 706, Paragraph 386 requires that there be "prompt revocation of access to protected information." Seven or 30 days would not be considered "prompt" by FERC.

One commenter commented that "next calendar day" for removal of access to BES Cyber System Information is too short a time span. The SDT points out that FERC Order 706 dictates prompt removal of access. The phrase "next business day" for example could mean substantially longer time periods over weekends and some holiday periods.

One commenter recommended the use of the word "repository" over "locations" in the requirement. The word "location" was chosen by the SDT to ensure there was no ambiguity within the requirement. Location is considered a general area, with multiple uses and is not limited to a specific function. A "repository" on the other hand, connotes specific use…for storage of BES Cyber Security Information. The use of location will help avoid any tendency toward requiring exclusivity of purpose and preclude potential violations.

One commenter commented that locations should be changed to designated repositories. The SDT believes that specifying a designated repository is less subject to interpretation and in most cases exempts portable equipment from being identified as a "location" in the event that NERC CIP information may be temporarily resident on such equipment. The SDT has retained the term "designated locations" since a location more often connotes multiple purposes. In contrast a repository, similar to location by definition, still carries connotations of a specified area, limited to a specific function. "Location" provides flexibility and designating locations removes incidental temporary storage on non-designated devices from the audit process.

Requirement Part 5.4 (formerly 7.4)

Some commenters would like to expand the applicability of requirement part 7.4 to include Medium Impact BES Cyber Systems. The SDT has carefully weighed the applicability of requirement parts throughout the family of Version 5 CIP standards, and, on balance, it believes that the levels of protection for Medium Impact BES Cyber Systems in other requirement parts throughout CIP-004-5 provide an appropriate balance in applying impact-based protections that are graduated between High Impact BES Cyber Systems and Medium Impact Cyber Systems.

One commenter suggested a revision for recovery of all information copied from repositories. The SDT notes that the requirements set out the requirements that must be part of the required processes. The SDT believes that the information protections in CIP-011-1 and the access requirements in CIP-004-5 adequately serve the purpose of protecting BES Cyber Systems while allowing sufficient flexibility to entities in implementing their processes or programs.

A few commenters recommended changing “Requirement parts 5.1 and 5.3 (formerly parts 7.1 and R7.3)” to “Requirement R5, Parts 5.1 and 5.3 (formerly R7 Parts 7.1 and 7.3.”)They also recommended changing the word “removal” to “revoke” for consistency with the requirement. Another commenter also suggested changing “revoke” to either remove or disable. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. The SDT has retained “removal” in part 5.1 along with a clarification which is provided in the requirement language. The SDT retained the term “revoked” in part 5.3 to conform to the overall R5 Requirement.

One commented that the phrase "revoke individual users accounts on BES Cyber Assets" should be changed to "revoke individual access to BES Cyber Assets." The commenter believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for the commenter’s field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays - Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay. It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time.

One comment suggested that in CIP-004 R5.4 (formerly R7.4): “For Termination actions, revoke the individuals user accounts on BES Cyber Assets...” to, for termination actions, revoke the individuals access to BES Cyber Assets...” The SDT has modified part 5.4 to read, “for termination actions, revoke the access to individual’s user accounts (unless already

revoked in accordance with requirement parts 5.1 or 5.3) (formerly parts 7.1 and 7.3) within 30 calendar days of the effective date of the termination action."

Some commenters disagreed with the statement that the word "revoke" in this case means to "delete" the user account from the system. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original Globally Unique Identifier (GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GUID will have been lost and difficult to track past account activity. This may be true for other operating systems as well. If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. The SDT has used the term revoke to essentially make an account "inactive". It does not delete the account. Also, requirement part 5.4 has been modified in the "Applicable Systems" section. It now includes only "High Impact BES Cyber Systems and Electronic Access Control or Monitoring Systems that are associated with High Impact BES Cyber Systems." Further, the requirement allows revocation of individual's user accounts within 30 days of the effective date of the termination action.

One commenter questioned that since there is no requirement for revocation of balance of access in 5.4 (formerly part 7.4) for Medium Impact BES Cyber Systems, is there a particular timeline required? The commenter recommended that a timeline be developed that provides auditable records for removing balance of access. In response, the SDT notes that requirement part 5.4 in the applicable systems does not include Medium Impact BES Cyber Systems. Under those circumstances the audit process would not be considering Medium Impact balance of access.

Requirement Part 7.5

One commenter points out that requirement part 5.5 (formerly part 7.5) only accounts for the 30 days within the requirement and not the 10 days after "extenuating operating circumstances". The SDT has provided measure in part 5.5 to cover that previous omission.

One commenter suggested that the second bullet of the example evidence for requirement part 5.5 (formerly part 7.5) should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. In response, the SDT has modified the measures to clarify that password resets must be completed within 30 days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.

One commenter recommended that requirement part 5.5 (formerly part 7.5) be revised to include both terminations and reassignments or transfers. The SDT has added part 5.5 to the requirement to cover the reassignments and transfers.

One commenter suggested that the quarterly review should be converted to a quarterly “cleanup” of individual user accounts and not be considered a violation, and the SDT notes that that a cleanup could certainly a way of identifying, assessing, and correcting any deficiencies, which now modifies “implement” in the main requirement (see summary response to common issues at the beginning of this document), and for that reason, the required performance of the requirement remains a review.

One commented that if an entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it should also apply to allow the Responsible Entity to determine and document that extenuating operating circumstances that can require a longer time period for revocation of access privileges. The SDT believes that since revoking physical and interactive remote (tier 1) access is typically a centralized and relatively uncomplicated process, that the time frames for completion are adequate. In addition, the FERC Order 706 requires “immediate” revocation of access. Providing a conditional caveat “for extenuating operating circumstances would in all probability meet with FERC resistance and result both in subjective application and interpretation.

One commenter questioned the need to modify passwords for shared user accounts if there is no corresponding requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known." The SDT has revised requirement part 5.5 (formerly part 7.5) to accommodate reassignments and transfers as well as termination actions. Requirement part 5.5 reads, “For reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.”

QUESTION B12 – CIP-005-5, R1:

If you disagree with the changes made in CIP-005-5, Requirement R1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language

SUMMARY:
Based on stakeholder comments, the SDT made significant changes to CIP-005-5 Requirement R1.

General Comments
One commenter suggested that the communications links between ESP's should be included and that all the External Routable Connectivity exclusions should be eliminated. In response, all BES Cyber Systems have been included within the scope of Version 5 and the blanket exemption filter in CIP-002-5 has been eliminated. The ERC filter is now used on individual requirements where routable connectivity is either needed to meet the intent of the requirement or in general there is insufficient risk from other forms of communication to enforce a mandatory and auditable requirement upon every instance in every registered entity. Communication links have been excluded from this body of standards from the beginning as it is a cyber asset focused standard, and the vast majority of cyber assets used in communications between ESP's are not within the control of the registered entities but are leased services from telecommunication providers.

A few commenters requested clarity around the inclusion of serial devices and another commenter also requested specific clarification concerning the extension of ESPs over large areas via serial communications along with a request for clarification of 'direct serial' used in the guidance. In response, the SDT has focused on the communications requirements of the standards for the highest risk forms of communication – routable protocol networks and public switched telephone network (PSTN) accessible dial-up connections. It is a vital point that all BES Cyber Assets, including all serial devices, are included in the standards and are subject to all the requirements in CIP-003-5 to CIP-011-1 except those where they are specifically excluded. CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication. As to the extension of ESPs over large areas via serial communications, the SDT notes that ESPs are for routable communication only and the SDT does not envision single BES Cyber Systems being defined in such a way that large geographical areas are involved. It is envisioned that a BES Cyber System would encompass cyber assets at a single site only – larger systems would be broken

at least into smaller systems by site. For example, a registered entity would not define all the components of an EMS including all field Remote Terminal Units (RTUs) as a single BES Cyber System. The components of that system at each location could be grouped together as the BES Cyber System for that location. Registered entities have great flexibility in their declaration of a BES Cyber System, but need to take into account ESPs and PSPs as well as all other applicable requirements as they do so. In response to the 'direct serial', that is used in the guidance as a term that refers to serial communications that is not routable protocol or dial-up in nature.

One commenter stated that clarity is needed concerning how wireless networks are impacted by CIP-005-5. In response, the SDT notes that these standards are at a higher and logical level and stay above the transport level. The SDT concentrated on protecting the BES Cyber Systems regardless of the physical transport in order to state the goal and also to future-proof the standards against an ever increasing variety of transports. Adequately addressing more detailed technical aspects would require standards per transport. However, the SDT does note that the radio/access point of a wireless network should be considered by the Responsible Entity to see if it should be included as an EAP.

Introduction Section

There was a comment that in the introduction section concerning exemptions (4.2.4) there is a reference to CIP-002-5 that should be CIP-005-5. In response, the SDT has made the change.

Background Section

One comment stated that the applicability of the background section does not address High Impact BES Cyber Systems with External Routable Connectivity and this is used in the standard. In response, the SDT agrees and has added the appropriate language which reads, "**High Impact Protected Cyber Systems with External Routable Connectivity** – Only applies to High Impact Protected Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the Protected Cyber System that cannot be directly accessed through External Routable Connectivity."

One comment read that Medium Impact BES Cyber Systems at Control Centers should be "associated with" instead of "located at". In response, the phrase 'located at' is used to appropriately limit the scope as the case could be made that

every Cyber Asset is ultimately 'associated with' a control center and could inappropriately identify every Cyber Asset as high impact.

One commenter stated that the section concerning Medium Impact BES Cyber Systems with External Routable Connectivity have the last sentence be deleted as it requires not treating the cyber system as one system, but as individual Cyber Assets. In response, there are several requirements (CIP-007-5 in particular) that do apply at the individual cyber asset level within a system and this sentence clarifies that for those requirements only those cyber assets within a system that have external routable connectivity are in scope if the requirement has this applicability.

Requirement Part 1.1

Many commenters commented that the applicability should include the ERC filter and thus remove the applicability language from the requirement itself and also make it parallel with R1.2, potentially even combining R1.1 and R1.2 into one. In response, the two requirements are purposely not parallel. R1.1 requires an ESP (a ***logical*** border) around every routable protocol network that contains a BES Cyber System even if it is an isolated network and has no external connectivity. The logical border (ESP) is used then as a boundary to define the 'associated Protected Cyber Assets' and raise the impact level of the included Cyber Assets to the 'high water mark' of the highest impact level system in the ESP. R1.2 is an additional requirement for those networks that have external routable connectivity to protect that external connectivity. In essence, Requirement R1.1 is the "identify your associated PCA's and adjust your impact levels" requirement. R1.2 is where external routable connectivity comes in and the logical border becomes more physical with the requirement of Electronic Access Points (EAPs).

Many commenters responded that the applicability needs to be removed from the requirement and the measure. Others commented that Associated Protected Cyber Assets should be included in the applicability as well. In response, the SDT has added the Associated Protected Cyber Assets to the applicable systems column.

There was one comment which stated that documentation on ESP's on isolated networks provides no reliability benefits. In response, the standards are concerned with all threat vectors, not just those originating from external networks. Portable media and insiders are two of many other threat vectors that can reach isolated networks. The SDT feels that knowing what all other network neighbors are on even isolated routable protocol networks containing a BES Cyber

System (the 'Associated Protected Cyber Assets') does have a reliability benefit. The logical border concept of the ESP also defines a 'trust zone' where all Cyber Assets sharing a network with a BES Cyber System need to be protected to equal levels, even on isolated networks.

One commenter stated that the measure should allow for documentation at the BES Cyber System level rather than the individual component level. In response, the SDT agrees and has made a change to the measure to allow documentation at either level.

One commenter requested clarification on whether ESPs are required for EACMs and PACMs. In response, the SDT clarifies that ESPs are not required on EACMs and notes that EAPs are EACMs and the standard avoids recursive effect of requiring ESPs around the cyber assets on the ESP. As for PACMs, the SDT notes that without an ability to make a distinction between "field-devices" (i.e. door readers, etc.) and "central servers", requiring ESPs would be problematic. The intent for protecting PACS is primarily through the CIP-007 requirements for authorization, access control, and logging and monitoring for these systems.

Requirement Part 1.2

One comment stated that the phrase "through the ESP" was redundant in light of the definition of External Routable Connectivity and should be deleted which would also eliminate the use of "through" twice in the existing requirement. In response, the SDT agrees and has deleted the phrase.

One commenter wrote that the measures should include a process to verify that all EAP's are identified as providing a network diagram is not sufficient. In response, the SDT notes that the requirement does not call for a verification process thus the measure should not imply that is a requirement. The requirement states the desired end goal and the entity is responsible for providing sufficient evidence. Network diagrams that depict all external routable communication paths with identified EAP's are listed as one possible example.

Several commenters stated that the applicability should be 'Associated PCA's with ERC'. In response, the SDT agrees and notes that the PCA for this requirement part are associated with high and medium impact BES Cyber Systems with External Routable Connectivity.

Requirement Part 1.3

A few commenters expressed concerns regarding the monitoring and documentation of all outbound traffic. Inbound only monitoring on PSPs is sufficient and suggest dropping the outbound on ESPs. In response, the SDT believes this is an essential element in combating today's electronic attacks and reiterates the following from the included guidance: "The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked."

Several commenters suggested that the applicability should be "Medium Impact BCS with ERC". In response, the SDT notes that the applicability is to EAPs that are associated with High or Medium Impact BES Cyber Systems specifically. If these applicable systems have no External Routable Connectivity, then they will have no EAPs and the requirement therefore does not apply to those systems.

One commenter suggested that the word "rationale" should be changed to "reason." In response, the SDT agrees as this makes the requirement language the same as that used in the measures and in the change rationale. The change has been made.

One commenter noted that tracking the rationale for 60000 ports is burdensome and asked that this be changed to allow for this on a class basis or 'criteria'. In response, the SDT notes the requirement does not require that all 65535 ports be documented as this is a 'deny by default' requirement and only the remaining open ports (those that 'grant access') should be documented. A necessary step in preventing rogue communications to or from a BES Cyber System is to know what the normal communications include and why they are needed.

Requirement Part 1.4

Multiple commenters stated that R1.4 is essentially the same as CIP-007-5 R5.1 and suggest that dial-up be added to CIP-007-5 R5.1 and R1.4 deleted to avoid potential double jeopardy. In response, the SDT notes that CIP-007 R5.1 is specific to user access, while CIP-005-5 R1.4 applies to any access including machine to machine. CIP-005 concerns the security of the 'network' level and requires that there be some form of authentication before a 'network' connection is established to the BES Cyber System. In essence, there should be some form of EAP-like functionality on dialups. Once a connection is made, then CIP-007 applies as we've moved from the 'network' level security to device level security and any user access has to be authenticated at the device.

One comment suggested that R1.4 should be deleted as it is included in R2. In response, the SDT notes that this requirement requires some form of authentication for all dialup connectivity regardless of whether it is machine or user based, while R2 only applies to 'Interactive Remote Access' which is user-based. The intent of R1.4 is that no BES Cyber System, which by definition can have a 15 minute impact on BES reliability, should be directly reachable by simply dialing a phone number, regardless of how it is intended to be used. Therefore R2 contains requirements that are in addition to R1.4 when the intent of the connection is user based Interactive Remote Access.

Several commenters asked if an entity has no dialup capability to applicable systems, are they required to have processes that would authenticate this access? The commenters suggested that the qualifier 'if applicable' be added. In response, the SDT notes the applicability column states that it only applies to systems "with dial-up connectivity" and therefore if an entity has no such systems, there are no systems to which this requirement applies and no process is required. The complete applicability of all requirements throughout the standards is contained within the applicability column and therefore every requirement in the standards has an implied 'if or where applicable' clause.

One commenter suggested that the "where technically feasible" clause should be changed to 'within system capabilities.' In response, the SDT notes that BES Cyber Systems, which by definition can have a 15 minute impact on BES reliability, should not be directly reachable by simply dialing a phone number. If that is not an inherent capability of the system,

then the SDT feels it necessary to add additional equipment with this capability to the system or file for a TFE so that a mitigation plan can be documented to handle the vulnerability.

One commenter suggested that 'where technically feasible' should be deleted. In response, the SDT notes the phrase is an indication of where TFE's may even be requested if the requirement cannot be met on a particular system. Since the SDT is not aware of all situations, it is felt that if an entity cannot meet this requirement on a system that they should be allowed to request a TFE and document a mitigation plan if the TFE is granted.

One commenter suggested that "Associated PCA's" should be added to the applicability. In response, the SDT agrees that any dialup connectivity to any system or Cyber Asset within the ESP, which by definition means the Cyber Asset is also routably connected to a BES Cyber System, should be included. The suggested change has been made.

Multiple commenters suggested that the term 'dial-up connectivity' should be defined to avoid future confusion and should include the notion of access from the PSTN. In response, the SDT is adding a proposed NERC Glossary definition of Dial-up Connectivity.

Requirement Part 1.5

Numerous commenters suggested that the measure only specifies IDS technology and should be made more generic to match the requirement. In response, the SDT agrees and has changed the measure to match the requirement, using IDS as one example.

There were multiple comments that detecting 'malicious' communications requires knowing the sender's intent. Malicious traffic may indeed appear normal. In response, the SDT is adding the phrase "known or suspected" to clarify that the intent is not to detect 100% of all malicious communications, but that communication that has attributes of known or suspected malicious communications.

Multiple commenters asked for clarity as to where the malicious communications inspection should occur and does the direction of the traffic matter. Another commenter stated that only one IDS could be utilized between all ESP's and the

Internet and one per EAP should not be required. In response, the SDT notes the applicability is set at the EAP level and therefore every EAP at Control Centers needs to be covered by the entity's method for detecting malicious communications. The specific architecture and placement is not prescribed. The SDT notes that since this applies to Control Centers, both inbound and outbound traffic should be subject to the detection and has added clarifying language to the standard. For example, if a BES Cyber System in a Control Center begins sending known malicious packets or attempting to communicate with known malicious 'command and control' hosts on the Internet that would warrant detection here and alerting through CIP-007 R4.

Several commenters suggested that the applicability should change to "Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers" as the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks. In response, the SDT notes that the requirement is applicable to EAPs and EAPs are only required where External Routable Connectivity is present, therefore isolated networks would not have EAPs and the requirement would not be applicable. However, isolated networks do have ESPs, so bringing the term ESP into the applicability may further confuse the issue.

There were several comments that raised a concern that the requirement is subjective and may not be feasible for encrypted traffic. In response, the SDT has written this requirement in response to FERC Order 706 and the directive to have two or more security measures at each ESP. The Order further clarifies that this is not simply redundant firewalls, but two separate security measures. The SDT has already reduced the subjectivity somewhat from 'two security measures' to 'detect malicious communications'. In today's technology, this would in most cases (but not all) involve the implementation of an Intrusion Detection System, but the SDT does not want to specify products or toolsets within the CIP standards to help future-proof the requirements. If a better toolset is available in the future that is not called "IDS" we would not want these standards to preclude the use of it, so we've deliberately used admittedly more subjective language ("a method for detecting…") in this case. As to the feasibility with encrypted communications, it is true that the methods will be 'blind' to the content of encrypted sessions but it is left to the entities to determine the relative value between maintaining true end-to-end encryption over terminating the encryption and inspecting the traffic at the ESP. The SDT notes that if the traffic is 'Interactive Remote Access', the encryption must terminate per R2 at the Intermediate Device which cannot reside within the ESP.

In the measures section, there were multiple comments to change the word “and” to “or” and to use bullets. In response, the SDT feels a generic paragraph is easier for clarity than bullets. The measure reads, “Examples of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.”

One commenter suggested that the phrase “where technically feasible” should be added to the requirement. In response, the SDT notes that this requirement is limited to Control Center environments. These are the highest risk locations and the SDT feels that in these instances some form of malicious communications detection (IDS) is always possible on routable protocol communications (EAP’s are required only on routable protocol communications).

One commenter stated that External Routable Connectivity should be added to the applicability. In response, the SDT notes that the applicability is to EAP’s which are only required for routable communication points.

Several commenters stated that detection is only one half of the issue and the standard needs to require addressing or mitigating the detected threat. In response, the SDT notes that EAP’s are EACM’s and are thus covered by CIP-007 R4’s Security Event Monitoring requirements and tie into CIP-008. Therefore the SDT feels that the ‘other half’ of the issue is covered by other standards. Xcel suggests that Intrusion Prevention Systems should be included instead of detection systems. In response, the SDT notes that in a control systems environment, the impact of preventing communications that may be the result of false positives may be greater than allowing the communication. Therefore we do not feel it necessary to require in a mandatory and enforceable manner that all suspected malicious communications should be prevented in all situations. That decision is best made by the Responsible Entity based on the specific situation and potential impacts.

One commenter suggested that the Medium Impact should be removed from the applicability as many of the Cyber Assets can’t perform this requirement. In response, the SDT notes that while many Cyber Assets in substations or plants (field locations) may not be able to perform this requirement, the Medium Impact systems are limited to those in Control Centers where the SDT feels the most risk is present and control center systems typically have the most capability to meet this requirement.

Guidance Section

One commenter stated that the guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP and an apparent conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP. In response, the SDT notes that the Intermediate Device is required only for human-machine interactive login sessions ("Interactive Remote Access") while the Requirement R1 is concerned with machine to machine sessions as well, which do not require an Intermediate Device. Requirement R2 builds upon Requirement R1.4 when the session meets the definition of Interactive Remote Access.

VRF/VSL Section

There was a comment on how the math is done on the VSL for Requirement R1. The SDT has modified the VSL for R1 to remove percentage calculations. We agree the percentage would be difficult to determine in most implementations. Furthermore, the FERC VSL Order addressing CIP Standards discourages specifying failure to document processes as a lower VSL than failure to implement.

There was a comment that suggested the VSL be medium for high impact and lower for medium impact. In response, the VRF by itself does not account for violations from different types of systems, but the SDT expects the impact level of the BES Cyber System to factor into the assessment of penalties.

One commenter suggested the ROP will need to change with changes to TFEs. Although the SDT does not draft Rules of Procedure changes, the SDT expects that this will be a part of the implementation of Version 5.

One commenter recommended modifying the first "Lower" to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, the commenter recommended moving this VSL to the "Severe" category. The lower VSL is intended for the situation where the entity has only failed to document the process(es). Where the entity has failed to implement one of the technology-based solutions listed in the table, those would fall in the moderate to severe categories based on number of technology-based solutions not implemented. The Lower VSL has been revised to clarify this further. Also by the FERC Guidelines for CIP standards, the failure to document processes should be the same level as the failure to implement a process. We have corrected the VSLs for R2.

One commenter recommended that the VSL for CIP-005-5 R2 VSLs be revised to address the approach to detect flaws; correct detected flaws expeditiously. Upon review of the approach to implement preventive, detective, and corrective controls, CIP-005-5 R2 was not identified as a requirement that would be appropriate for this approach. Therefore, the VSL was not modified as requested.

One commenter agreed that the VRF should be medium for the high impact BES Cyber Systems but that the VRF should be lower for the medium impact BES Cyber Systems. In response, VRFs are assigned for an entire requirement and are not assigned to the underlying sub-requirements or parts.

QUESTION B13 – CIP-005-5, R2:

If you disagree with the changes made in CIP-005-5, Requirement R2 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, the SDT has made significant changes to CIP-005-5 Requirement R2. The explanations below describe the changes made based on stakeholder comments – the SDT made other minor edits for improved clarity.

TFE Relevance
In response to concerns that the phrase "where technically feasible" should be removed to eliminate reference of maintaining the TFE process, the SDT notes that TFEs will continue to be used in appropriate requirements unless and until such time that the NERC ROP is modified to address exceptional circumstances. The SDT has reviewed each use of a TFE throughout the CIP Version 5 standards very carefully and specifically, and in each instance where that phrase is used, the SDT understands that there may be circumstances where it could be necessary for an entity.

In response to multiple comments that the applicability of TFEs is not clear within the TFE language included in the overall Requirement language, the SDT has moved the TFE language to the table elements.

Applicability
Several comments stated that instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". This is a valid concern, and in response, the SDT has added the language to the applicability section of the table.

There was also a comment that the requirement should apply to Physical Access Control Systems and systems serving as ESP Access Points. In response, the SDT believes that since these systems generally do not reside within the ESP of a BES Cyber Asset, it would not be appropriate to apply these Requirements to those Cyber Asset types.

Requirement Part 2.1: Intermediate Device
There was a comment requesting that the reference to Intermediate Device be removed from the requirement. In response, the SDT notes that the Intermediate Device is a defined term that is only used within this one requirement. The device functionality is necessary to ensure that proper protections are put in place for Interactive Remote Access

sessions. The use of Intermediate Devices allow the client machine to exchange data to a Cyber Asset within an ESP without making direct communication and opening the Cyber Asset to vulnerabilities of the client machine.

Several commenters requested improvements to the language in requirement part 2.1 to clarify that a Cyber Asset cannot initiate Interactive Remote Access. In response, the SDT has clarified the language to address this concern by specifying use of an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. However, the language was not modified to address the person using Interactive Remote Access since the requirement is intended to provide protection from malicious software and communications.

Commenters requested clarification on the location of an Intermediate Device and whether an Intermediate Device can also be an EAP. In response, the SDT notes that the definition of Intermediate Device has only one restriction on the location of the Intermediate Device and that is that the Intermediate Device must not reside in an ESP. Other requirements of the Intermediate Device remain flexible to allow the entity to implement a solution that best meets their needs.

Requirement Part 2.2: Encryption

Several commenters requested that the information regarding the purpose of encryption be removed and added to guidance. The use of "in order to protect the confidentiality and integrity of each Interactive Remote Access session" was intended to help clarify the encryption means that were appropriate.This language has been removed, allowing the Responsible Entity the flexibility to implement the level of encryption appropriate to their organization. Additional references regarding encryption are available in the *Guidance for Secure Interactive Remote Access* document. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Several commenters requested clarification on the termination point of required encryption. The requirement states the encryption is to terminate at an Intermediate Device. The Intermediate Device may be one or more assets performing the required functions. Encryption should not be perfromed within the Electronic Security Perimeter due to the negative impact on the monitoring for malicious or suspicous communications.

Requirement Part 2.3: Multi-Factor Authentication

Several commenters requested that the examples of multi-factor authorization be removed from the requirements. In response, the SDT has removed the examples from this requirement part, and the requirement part simply reads, "Require multi-factor authentication for all Interactive Remote Access sessions."

Several comments recommended more flexibility regarding the use of multi-factor authentication to allow for future technology changes without a Standards update. In response, the SDT has made this change within the measure so that it is listed as an example, but the requirement can account for future technology changes as commenters suggest.

Many comments requested clarification as to where the multi-factor authentication needs to take place. In response, the SDT has modified the Requirement to state that multi-factor authentication to the Intermediate Device is required for all Interactive Remote Access sessions. Furthermore, the definition of Intermediate Device specifies that access control be performed at the Intermediate Device. The Intermediate Device may be one or more assets performing the required functions.

QUESTION B17 – CIP-006-5:

If you disagree with the changes made to CIP-006-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, there were changes to the applicability section, the requirement parts for added clarity, and removal of unnecessary requirement parts that were documentation related.

General
The "identifies, assesses, and corrects deficiencies" language has been added to Requirement R1 and Requirement R2 since these formerly were zero defect requirements. The SDT believes this is an improvement in the compliance process.

The applicability section was renamed to applicable systems to help clarify the scope of that requirement. Also, the applicable systems entries in each table were reviewed to ensure it matched the requirement language for consistency within this standard and with the other CIP Version 5 standards.

The SDT made changes to table R1 to address concerns on the applicability of requirement parts 1.1, 1.2, and 1.3 that had layered versus exclusive applicability. The table no longer uses layered applicability to be consistent with tables in other CIP standards.

The wording of requirement parts 1.2 and 1.3 has been revised to clarify unescorted access is restricted to those authorized for such access, but escorted individuals can enter a Physical Security Perimeter (PSP).

There was consideration of combining monitoring and issuing an alarm/alert into a single table entry, but these are separate actions and needed separate table entries. Even with separate table entries, each is part of a single requirement.

The SDT has removed the 99.9% availability requirement and requirement part 3.2 to document outages for physical access control, logging, and alerting systems. The Physical Security Plan(s) should address how an entity deals with unavailability of these systems.

Requirement parts 1.4 and 1.5 have been modified to remove the reference to circumvention of a control. The new language is monitoring and issuing alarms/alerts for detected access through a physical access point into a PSP. Designation of physical access points to the PSP should be noted in the physical security plan(s).

A PACS is not required to be within a PSP. Unauthorized physical access is to be restricted. The alarm or alert is for detection of unauthorized physical access similar to the language in requirement parts 1.4 and 1.5, although a PSP is not required.

Data retention requirements that differ from the compliance data retention requirements have explicit language in the requirement table. For example, the retention requirement of 90 days for retention of physical access entry logs is specified in requirement part 1.9.

CIP 006 Requirement R1.3

Language has been added to this table, *"… two or more different physical access controls to collectively allow unescorted physical access into Physical Security Perimeters,"* to clarify that two completely independent physical access control systems are not required. For example, a card key and biometric scan using the same Physical Access Control System for validation is acceptable. Also, the SDT has chosen not to use the words "two factor authentication" since, for example, some field locations could use two separate locks. Further, the SDT believes there may be some locations, particularly for field assets, that may not permit two or more different controls, so the TFE clause remains.

CIP 006 Requirement R1.5 & R1.7

The SDT heard the concerns expressed by industry about when the 15-minute clock begins. The language in the standard has been changed to begin once detected. Also, the language referring to the Cyber Security Incident Response Plan remains as that plan could cover physical incidents related to access to cyber assets.

CIP 006 Requirement R1.8

The SDT has chosen to retain the phrase *"… through automated means or by personnel who control entry."* It confirms in the requirement that a person cannot self-log their entry into a Physical Security Perimeter and that the use of a guard is an acceptable method to log entry.

CIP-006 Requirement R2

This requirement does not state that the visitor control program(s) has to be a standalone document/program. If the entity chooses to include the required language within the Physical Security Plan, that is acceptable.

CIP 006 Requirement R2.1

The language in the parenthetical "*(individuals who are known or guests, and not authorized for unescorted physical access)"* has been removed. A "visitor" is anyone who does not have authorized unescorted physical access inside the PSP. This could include employees, contractors, service vendors, etc. The measure indicates that evidence may include documentation of the visitor control program and visitor logs. There is no reference to "proof" that a visitor was continuously escorted.

CIP-006 Requirement R2.2

The language was edited to correct the implication that a visitor exits to a PSP. Also, the measure was modified to better match with the requirement.

CIP-006 Requirement R3

The SDT considered the suggestion to remove the term "hardware" from the phrase "… locally mounted hardware and devices…" used throughout this requirement. This same phrase has been used in previous versions and is understood to exclude hardware such as door hinges, screws, etc. Also, there is new language in the background section regarding applicable systems that provides additional information on locally mounted hardware or devices.

CIP-006 Requirement R3.1

The SDT believes the key role played by the PACS and associated hardware and devices in protecting High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity warrants a 24-month testing cycle. PACS used for Medium Impact BES Cyber Systems without External Routable Connectivity do not have this requirement.

QUESTION B23 – CIP-007-5, R1, R2, R3 or R4:

If you disagree with the changes made in CIP-007-5, Requirement R1, R2, R3 or R4 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments,

General Comments
One entity commented that there is a reference in the 4.2.4 exemptions section that refers to CIP-002 but should refer to CIP-007. In response, the SDT agrees and has made the change.

Several commenters commented that either all VSLs or VSLs for certain requirements should be based on percentage of cyber assets missed. Using percentages based on Cyber Assets on CIP-007-5 Requirements is problematic because Requirements do not have a singular mapping to assets. Also, it is possible for a single Cyber Asset to have multiple violations.

One commented that all Severe VSLs should state the phrase "failed to implement one or more documented." The SDT reviewed this suggestion, and "did not implement" as the SDT proposes is consistent with the SDT's intent.

Requirement R1 General Comments
One commenter suggested that the rationale section for Requirement R1 needs to include physical ports. In response, the SDT agrees and has added this to the rationale.

Several commenters stated that throughout Requirement R1, the applicability for Medium impact should be limited to Medium Impact with external routable connectivity (ERC). In response, the SDT notes that Requirement R1.1 which applies to network accessible ports is already limited to those systems with ERC. Requirement R1.2 refers to physical ports that could be used by someone physically present to inadvertently or intentionally compromise a BES Cyber System. In this case, ERC does not matter and the SDT believes the ERC exclusion should not be considered in this case.

There were a few suggestions that the High Impact systems should include the ERC filter as well. In response, the SDT notes that since Version 1 of the CIP-002 standard, lack of external routable (or dial-up) connectivity has been a blanket exemption everywhere except Control Centers, where even standalone networks were still to be considered as Critical Cyber Assets. Since High Impact in Version 5 refers to Control Centers, the SDT cannot 'go backwards' without sufficient justification, which we believe is absent.

One commenter suggested that the words "and Services" should be dropped from the title as the requirement concerns only network ports. In response, the SDT notes that ports are opened by services and that typically a port is disabled or closed by disabling the corresponding service. The requirement also allows for services that use wide ranges of dynamic ports that need to be enabled to be documented as the service name rather than a dynamic port range. Therefore the SDT believes the 'and Services' is appropriate.

Several commenters stated that the Requirement R1 measures may also include rationale as to why ports are necessary or clarify in the requirement. In response the SDT agrees and has added a specific measure for documentation of the need for all enabled ports.

Requirement Part 1.1

One commenter suggested that the phrase "ports or services" should be "ports and services". In response, the SDT notes that the use of the word "or" is intentional to allow for circumstances where a Cyber Asset uses one service that is on one port, another service that uses a range of ports, or a service that uses dynamic ports without a defined range (e.g. may use anything over 1024). The entity should be allowed to document the enabled single ports, port ranges, or in the case of the dynamic ports, the service that is enabled. Therefore the SDT feels the word "or" is appropriate.

Two commenters suggested that the sentence in the guidance concerning cyber assets that allow for no port management and therefore all open ports are deemed 'needed' should be part of the requirement. In response, the SDT agrees and has moved the sentence to the requirement.

One commenter suggested that the phrase 'where technically feasible' should be replaced with 'within device capabilities'. In response, the SDT notes that devices that do not allow for port management will have their ports determined as 'needed' thus the TFE will be seldom used. However, the SDT wanted to allow for entities to request a TFE for any special cases.

One commenter suggested that the requirement should consider more than listening ports but should also include unexpected connected ports making outbound connections. In response, the SDT notes that this risk is covered at one level by CIP-005's new outbound rule requirement. The SDT also notes that this requirement requires evidence of a known port configuration for the cyber asset and it is unclear how an entity could perform this for 'unexpected' ports.

Several commenters asked for clarification as to how "associated PCA's" applies and is not an independent set of individual assets. In response, the SDT notes that most of CIP-007, and Requirement R1 in particular, must be implemented at an individual cyber asset level and the requirement thus starts with 'For applicable Cyber Assets'. Ports and services are enabled or disabled on individual Cyber Assets and most of CIP-007 can't be done at a 'system' level but at a Cyber Asset level. For example, if an entity does not need telnet service, then the only way to prove that it has been disabled is on an individual Cyber Asset basis – ports and services are by nature not implemented on a 'group' of Cyber Assets but on individual Cyber Assets.

FMPA and LCEC commented that the SDT should add the phrase "that initiate or receive network communications" after the word "services" or delete services and let ports handle it. In response, the SDT notes that the services is part of "port ranges or services" and are two levels at which the entity can document the enabled logical network accessible ports. This was added primarily to handle dynamic ports. Some systems will use a particular dynamic port out of a small range of ports and documenting that range is acceptable. Other services may pick a dynamic port out of all the high ports (any port between 1024 and 65535 e.g. RPC) and the SDT's intent is to allow for documenting the need at the service name level.

Some commenters suggested that clarification that the Responsible Entity determines the need of port should be included. In response, the SDT agrees and has added clarifying language.

One commenter suggested that the phrase "enable only logical network accessible ports needed" should be "enable only required logical network accessible ports." In response, the SDT notes that the intent is to document the business or technical justification for all open ports. In previous drafts, numerous comments were received to change the word "justification" to "need", which was accepted by the SDT. The SDT also notes there is a difference in "required" and "needed" and thinks "needed" is a more appropriate term due to instances where a Cyber Asset may be fully able to perform its basic function without the port enabled (thus the port is not technically "required"), but the port is "needed" for other purposes. Similarly, KCPL commented that the "needed" should be changed to "approved" for clarity. In

response, the SDT notes that these ports are part of the tracked baseline configuration in CIP-010 and approvals occur there. The SDT has therefore not brought in the approval process into CIP-007.

One commenter suggested commented that 'listening' should be replaced with 'enabled'. In response, the SDT believes the term 'listening' is more descriptive as the intended scope is those ports that can actually be reached from the network. A port can be 'enabled' at one level (a config file), but blocked by other means lower in the OS (e.g. TCP_Wrappers) such that it is not actually 'listening'. The end goal is blocking accessibility from the network to unneeded ports and the SDT believes 'listening' better captures that goal.

One commenter suggested that a fourth bullet should be added to the measures to address CIP-005-4 R2.2: Listing of access points to the ESPs, including configuration of ports and services, individually or by specified grouping. In response, the SDT agrees that EAP's should be highlighted and has added this to the first bullet point.

One commenter suggested that the measure should add the phrase "or class of Cyber assets" to the second bullet. In response, the SDT agrees and has added the phrase "individually or by group" to the bullet point.

One commenter suggested that the first bullet under the measures should be deleted as it doesn't meet the requirement. In response, the SDT agrees that a simple listing of port need is not sufficient to meet the requirement and has replaced that measure with the phrase "Documentation of the need for all enabled ports individually or by group".

One commenter suggested that the list of listening ports could be a source of double jeopardy with CIP-010's baseline configuration requirements. In response, the SDT notes that the requirement is concerned only with the enabling of only needed ports irrespective of any documentation. The list of enabled ports is a requirement in the baseline configuration requirement in CIP-010. The SDT believes that failing to maintain the baseline configuration and failing to actually go to a Cyber Asset and disable unneeded ports are two different requirement violations. The measures for this requirement refer to listings of ports as evidence, but that evidence could be the same evidence required for CIP-010. Being able to utilize a single piece of evidence for proof of compliance with two different requirements is not double jeopardy.

There was a commenter who suggested that instead of the phrase 'class of cyber asset' the language from CIP-010 should be used. Also, the requirements should address justification of enabled ports. In response, the SDT agrees and notes that justification is addressed by the phrase 'needed by the Responsible Entity' and the measure has been changed to

now call for documentation of the need for all enabled ports. The SDT also agrees with the 'class of cyber asset' comment and has incorporated the language 'individually or by group' from CIP-010 as suggested.

One commenter suggested that the reference to CIP-005-5 R1 to protect the network in the guidance should be deleted. In response, the SDT agrees and has deleted the language, leaving only the clarification that blocking ports at the ESP does not substitute for the device level requirement.

One commenter suggested that the guidance should allow for disabling ports 'inline in a non-bypassable manner'. In response, the SDT agreed with this in the draft 1 comment phase and made that change between drafts 1 and 2.

Requirement Part 1.2

There was a comment that the text should be revised to begin with the phrase "Have methods to protect against..." since the VSL is for not having methods. In response, the SDT notes that the overall Requirement R1 is to "implement documented processes" and changing this to have methods would add another level of abstraction such that the overall requirement would be "implement documented processes to have methods to protect."

A commenter suggested that this requirement should be replaced with a 'implement a policy' type requirement. In response, the SDT does not believe that a policy only requirement would meet the FERC directive in Docket No. RD10-3-000 of March 18, 2010, which is the genesis of this requirement.

Several commenters suggested that signage is a weak control that does not provide adequate protection. In response, the SDT notes that signage was never meant to be a preventative control against intruders. Signage is indeed a directive control, not a preventative one. However, with a defense-in-depth posture, different layers and types of controls are required throughout the standard with this providing another layer for depth in Control Center environments. The industry has made several comments as to the other preventative and detective measures that are required before physical access to a physical port is ever achieved. Once physical access has been achieved through the other preventative and detective measures by authorized personnel, a directive control that outlines proper behavior as a last line of defense is appropriate in these highest risk areas. In essence, signage would be used to remind authorized users to "think before you plug anything into one of these systems" which is the intent. This control is not designed primarily for intruders, but for example the authorized employee who plugs his infected smart phone into an operator console USB port "just to charge the battery".

Several commenters stated that this requirement needs further justification for its existence. In response, the SDT notes that this requirement was added to address FERC's Docket No. RD10-3-000 of March 18, 2010 which states, "However, like NERC, we are concerned that neither CIP-007-2 in particular, nor the CIP reliability standards in general, adequately address technical opportunities to mitigate risks associated with unused physical ports. The practice of disabling or otherwise securing unused physical ports is a basic and integral component of sound defense-in-depth cyber security practices, yet it is absent from the current reliability standards. The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP reliability standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."

One commenter stated that entities may not be able to block physical ports based on usage using the example of unplugging a USB keyboard or mouse and using a thumb drive in that enabled port. In response, the SDT notes the requirement is to "protect against the use" and purposefully does not use the verb "prevent" in recognition that the control is not effective in prevention in many cases as the industry has pointed out. The intent of the requirement is not to be a 100% preventative control, but is a last measure in a defense in depth layered control environment to make personnel think before attaching to a BES Cyber System in the highest risk areas.

There was a comment that this requirement should be limited to network ports as portable media is handled elsewhere. In response, the SDT notes that BES Cyber System Information on portable media is handled elsewhere, not the portable media itself. Portable media is becoming a primary means of entry into entities and the SDT believes that to meet FERC's intent, portable media and console command ports should remain in scope.

One commeneter asked for clarity on whether the disabling of physical ports could potentially reclassify a device that would otherwise be considered a BES Cyber System. For instance, if a routable device had all of its physical network ports blocked then what otherwise might be a routable device cannot route. In response, the SDT notes that the ability to communicate outside of itself is not a determining factor as to whether a Cyber Asset is or is not a BES Cyber Asset or BES Cyber System; the Cyber Asset's function as it pertains to BES reliability determines that. So although a Cyber Asset may indeed be a BES Cyber Asset, if all communication ports are disabled then the BES Cyber Asset would have no External Routable Connectivity or dial-up connectivity and thus none of the requirements which have that condition in the applicability column would apply. The specific example of the programmable television monitor provided would have to be determined by the Responsible Entity as to whether the monitor met the definition of a BES Cyber Asset. If the

monitor is not a BES Cyber Asset, then it is not a part of a BES Cyber System. The SDT notes that BES Cyber Systems consist of one or more BES Cyber Assets, not every programmable electronic device.

There was a comment asking for clarity as to whether ports could be protected via a common method or must the protections be per port. In response, the SDT notes that the requirement is not prescriptive in this manner and does not preclude either as the measures and guidance allow for directive measures.

One commenter stated that the word "unnecessary" should be changed to "not required". In response, the SDT is allowing for slightly more flexibility than is denoted by terms such as "required" or "not required". A port may be "necessary" for some use of the entity but not technically "required" for the operation of the device.

Requirement R2 General Comments

Several respondents commented that patch management should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while managing patches on all Cyber Assets is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry focus to the lowest impact assets if we don't maintain that balance. The SDT also believes that many devices will probably have some portion of the population declared as medium impact and thus many entities will need to handle any vulnerabilities on those devices and oftentimes will just patch all devices of that type.

There were many commenters that suggested that all sub requirements should have the applicability changed to medium impact with ERC. In response, the SDT notes that managing security patches or otherwise mitigating the vulnerabilities the patches address is a core activity in protecting our critical infrastructure. While external routable connectivity does increase the risk, the lack thereof does not reduce it to an acceptable level as many threats enter the environment by other means such as thumb drives, laptops, smart phones, etc. The SDT does not believe we can adequately protect the infrastructure if we only concern ourselves with patching devices with external connectivity due to the remaining threat vectors. However, the SDT does understand the evidence burden and has made changes to this requirement to reduce that burden. The requirement now allows entities to focus on a monthly 'batch' cycle of patches rather than tracking timelines for every individual patch, and no documented mitigation plans are needed if patches are installed within the 70 day time period. It is the SDT's intent that these and other changes in this requirement will relieve the documentation

burden while still requiring the performance of this basic security activity. The essence of this requirement is to have the industry watching and aware of vulnerabilities in their BES Cyber Systems, whether they are routably connected or not, and mitigating those vulnerabilities. Many patches may address vulnerabilities that the entity has already mitigated through existing means and require no action. In fact, it is expected that the lack of external routable connectivity would be used as a major factor in many applicability decisions and/or mitigation plans where that is the case.

Several commenters stated that the requirement should not require a documented remediation plan for every patch, but outline a standard patch mgt process with documented deviations. In response, the SDT agrees and has modified part 2.3 to allow for this.

There were a couple of comments that clarification is needed on failed patches installed well after the 60 days but according to the entity's plan. In response, the SDT has modified the requirements such that a plan may be revised (see requirement part 2.4).

One commenter suggested that the word "processes" should be changed to "program" throughout R2 so it aligns with 2.1. In response, the SDT agrees the terms should match, but notes that Requirement R2 (above the tables) uses the word "processes" and has changed the term "program" in 2.1 to "process" so that the entire requirement uses the same term.

One commenter stated that the requirement in essence rewards obsolescence and never requires upgrading to a patchable system. In response, the SDT notes that the standard's intent is to secure the infrastructure that is in place without requiring equipment upgrades of currently functional equipment solely for security purposes. Cyber security risks are one factor in the decision to upgrade. The SDT also notes that cyber risk is determined by many factors, and older equipment could actually have a lower cyber security risk. These decisions are best left to the Responsible Entity to make based on the specific circumstances rather than mandated unilaterally in a cyber security standard.

There was a comment that clarity should be provided on what constitutes a "security patch" and what is "updateable". In response, the SDT agrees and has added clarifying sentences to the guidance section of the standard for part 2.1.

Requirement Part 2.1

Multiple comments stated that the phrase "security patches" should be changed to "patches and security upgrades". In response, the SDT is concerned with expanding the scope beyond patches to words such as upgrades or updates. The

SDT does not desire to create the situation where a vendor creates a new version of their software, mentions something new about security in the new version, and suddenly everyone is under mandatory compliance obligation to either upgrade or create a plan. Cyber security features are one component of an upgrade decision. The SDT believes that keeping this requirement to the word "patches", which are fixes to their existing version, is what should be mandatory. The SDT also notes that patches are a fix to a specific vulnerability, which is what the requirement is based upon as it is under obligation to mitigate the vulnerability.

One commenter suggested that applicability and compensating measures should be determined based on original source of patch (e.g. Microsoft) rather than the SCADA vendor. In response, the SDT agrees that this is a best practice so that vulnerabilities may be mitigated in the shortest timeframe possible, even before the patch is certified by the SCADA vendor. The SDT notes that the provided example is the most obvious one with Microsoft, however if included in a mandatory and auditable environment this would extend to the seemingly unlimited non-obvious situations where an entity buys a system from vendor 'X', but vendor 'X' is using software components from 20 other vendors. The entity does not know all the original sources of all components of the system. Situations such as what is the RTOS (Real Time Operating System) involved in a particular digital relay would arise, and why didn't the entity track the vulnerability info for that RTOS directly from that vendor rather than the relay vendor's firmware levels? The entity is not a direct customer of that RTOS vendor and may not have access to that information. In summary, while the SDT believes this is a best practice in some situations, making it mandatory and auditable in every situation is not something that entities can comply with as the standard expands in scope to every BES Cyber Asset in the field.

There was a recommendation that more guidance is needed on appropriate patch sources. In response, the SDT notes that the 'appropriate sources' was added to this requirement from Version 4 so that a definite start date for the evaluation timeframe could be determined. The appropriate source is going to be dependent on the situation. If the Responsible Entity has a control system from vendor who invalidates support contracts if the system is patched outside of their approval, then the vendor should be the appropriate source. If the system were custom built by the Responsible Entity, then the vendor for each of the components used to build the system would be the appropriate source.

One commenter recommended that the program should be specified in Requirement R2 and not Requirement R2.1 as a process does not include a program. In response, the SDT agrees and has changed the word "program" in R2.1 to "process" so that it agrees with Requirement R2.

Some commenters said that the process should include a periodic review (monthly) of all patch sources rather than maintaining timeframes per patch. In response, the SDT agrees and has made changes to the language to incorporate this concept.

There was a comment that the requirement should insure that documentation of sources is a onetime exercise unless new software is added to the baseline. In response, the SDT agrees and has clarified this in the guidance section of the standard.

Requirement Part 2.2
Numerous commenters suggested a change to 35 calendar days to allow for a monthly cycle. In response, the SDT agrees and has made the suggested change.

One commenter requested that the guideline states that entities are allowed to evaluate and accept risk which FERC Order 706 disallows. In response, the SDT agrees and has modified the guidance.

There were a few commenters that requested additional clarity on what the term 'applicability' means. In response, the SDT agrees and has added clarification to the guidance section.

One commenter suggested alternative wording, "Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in requirement part 2.1. The assessment must include determination of the applicability of each patch to the entity's specific environment and systems as well as reason for a patch's non-applicability." In response, the SDT has modified this requirement to incorporate a monthly review of the patch sources, but has chosen not to get more prescriptive with the term applicability within the requirement. The SDT believes that evaluating applicability necessarily means that the entity will be documenting the final determination for their environment.

Requirement Part 2.3
Some commenters proposed changes to the timeframe and process such that it would allow 60 days and have no remediation plan required if the patch is installed within 60 days. In response, the SDT agrees and has modified the requirement so that applying the patch or creating or revising a mitigation plan are all choices the entity can take within the second 35 day period. The SDT notes, however, that the timeframe is 70 days total with 35 days for tracking and

determining applicability and 35 days for either installing or determining the mitigation plan. It is not 35 days plus an additional 60 days for the second step.

There were multiple comments that the word "dated" should be revised since it is open-ended. In response the SDT believes the word "dated" is necessary and the requirement would be open-ended if it had no date required for the plan. The date of the plan in requirement part 2.3 is what part 2.4 depends upon.

One commenter stated that the requirement was overly burdensome due to the sheer number of patches. In response, the SDT notes that due to the burden the auditable cyber assets are limited to High and Medium Impact Systems and associated systems. The SDT has changed the requirement so that the tracking can be on a monthly basis for all patches released that month rather than on an individual patch basis, which should help.

Some commenters suggested that specificity is needed as to a maximum timeframe. It is compliant with the requirement to state a timeframe of the phrase "End of Life Upgrade". In response, the SDT has had numerous discussions around this issue. The SDT has decided that the reliability risk of putting prescriptive and mandatory timeframes for patching outweigh the risks of having an open-ended patching timeframe. There are numerous reasons. One reason is the industry goes through periods of time during seasons of the year that we refer to as "nobody is touching nothing" mode because the risk of any change to equipment or systems invokes an availability risk when the asset is depended upon the most. Tripping a generating unit on a 100-degree day because a standard said we were out of time to patch it to fix some minor issue is not acceptable. Another reason is we are in a largely legacy equipment environment as this standard expands outside of control centers where there are no patch management solutions. Upgrading the firmware in thousands of digital relays is something that must be planned and executed very cautiously. Firmware based devices will require planned outages for patches and present the risk of "bricking" the asset. So for these and other reasons, the SDT has decided the implementation timeframe is best left up to the entity rather than enforcing some arbitrary timeframe. The requirement is that they have a dated plan and must work towards that plan. We believe this is the best tradeoff between the risk of someone exploiting a vulnerability and the inherent risk of changing code in devices where availability is paramount. If the SDT set a maximum timeframe to handle these sorts of cases, we would have numerous comments about how the timeframe is too long. We believe that setting a timeframe to handle these cases would actually draw a line in the sand that would have the unintended consequence of all patch timeframes moving toward that timeframe. If the entity has to set its own timeframe and defend it, then they won't all tend to move towards the maximum timeframe specified in the requirement.

Two commenters suggested that the requirement should allow for revision to an existing plan. In response, the SDT agrees and has changed the language to allow for revisions.

There were a few recommendations that the word “exposed” should be “addressed”. In response, the SDT agrees and has made the change.

There was a comment that a potential double jeopardy issue exists between requirement parts 2.2 and 2.3. In response, the SDT has made numerous changes to these requirements and believes that any double jeopardy issues have been addressed.

One commenter stated that an evaluation of the language in the change rationale should be done to determine what needs to move into the requirement itself. In response, the SDT believes that what remains in the rationale is rationale and has no actionable requirements that could be moved to the requirement itself. However the SDT agrees the language in the rationale should be preserved and has moved it to the guidance section as well.

There was a comment that addressing the vulnerability could be entirely dependent on vendor’s patch development timeframe to address a vulnerability. In response, the SDT notes that the process begins upon the release of the patch from the source identified by the Responsible Entity. The patch has been developed and is available before the process required in R2.2 and following starts.

One commenter asked about the need for TFEs where patches cannot be applied. In response, the SDT notes the intent is that TFEs are not required at any step in the process. The process has been designed to alleviate the need and guidance has been included as well to address this issue.

There was a comment that the first sentence in the guidelines for Requirement R2.3 is a restatement with different wording and may imply other requirements. In response, the SDT agrees and has changed the guidance to more closely match the requirement.

Requirement Part 2.4

Multiple commenters stated that the plans should allow for revision in other than CIP Exceptional Circumstances before the timeframe expires. In response, the SDT agrees and has added the ability to revise the plan if done through an approved process such that the revision or extension is approved by the CIP Senior Manager or delegate.

An issue was raised that there is a potential double jeopardy issue as 2.4 duplicates Requirement R2 where 'implement' is required. In response, the SDT does not believe that a double jeopardy issue exists because the implement in the overall requirement is for the patch management process, whereas the implement in R2.4 is for the individual patch. If R2.4 does not have an implement requirement at the patch level, then the 'implement' in the overall requirement only applies to drafting a plan.

One commenter suggested that guidance should be offered on how much information is expected to demonstrate implementation. In response, the SDT notes that example measures are provided and that the requirement is for the implementation of a mitigation plan, thus the measures would be records of the implementation of the plan. The plan may include such things as installing the patch and the measure would be a record of the installation, or the plan may include the disabling of an affected service, or the adding of a signature to an IDS, or a change to a host based firewall to handle the vulnerability and the measure would be the record of the completion of these changes.

There was a comment that the change rationale is from 2.2 and doesn't address 2.4. In response, the SDT agrees and has updated the rationale to match the changes in the requirement.

To address the comments that bullet 2 of the measure should read "records of vendor recommended or other appropriate mitigations" the SDT agrees and has added "or other appropriate" to the measure.

Requirement R2 VSL

One commented that the R2 and R3 VSLs increment by different ranges. In response, R3 has been modified to remove specific timeframes in the Requirement and the VSL has removed the referenced increments.

Requirement R3 General Comments

One commenter requested that the requirement should apply to all applicable Cyber Assets including all Low Impact. In response, the SDT believes that while this is a best practice, making this a mandatory and auditable requirement would divert the industry's attention to managing an onerous burden of records on orders of magnitude more devices at the lowest impact level. The SDT has been careful to balance what is absolutely required in a mandatory and enforceable manner and the burden of proof such a change would entail with maintaining a high degree of industry focus on the higher risk assets. If we overburden the Low impact classes, it would be easy to divert an inordinate amount of industry

focus to the lowest impact assets if we don't maintain that balance. The SDT believes that keeping the requirements on Low impact systems at a programmatic level rather than a device level is the only way to keep that balance.

Multiple commenters suggested that the applicability should change to all medium impact with ERC. In response, the SDT disagrees because the threat of malicious code is not limited to introduction through external routable connectivity. The threat of malicious code is arguably higher from portable media, temporarily connected cyber assets (vendor laptops, etc) and inadvertent insider actions.

Requirement Part 3.1

There were a few comments which stated that the intent should be clarified and suggested language includes "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used on every single Cyber Asset." In response, the SDT notes that the applicability is at the 'system' level and the intent is to keep it at that level as this is a requirement where the 'system' level is beneficial. Therefore, the SDT believes it is best to not fill the requirement with language at an individual cyber asset level.

There were several concerns that Requirements R3.1 and R3.2 are too vague. In response, the SDT notes that the requirements are indeed written at a very high level but the SDT believes it is necessarily so. Malicious code protection is at the 'forefront of the fight' and is rapidly evolving and changing to match the ever changing and morphing threat. The SDT believes the protection of our infrastructure can be better accomplished if we do not have prescriptive technical methods detailed in this requirement. This could have the unintended effect in the future of stifling innovation and the use of new and better tools that would provide better protection but not be compliant with what the SDT would specify today. It does not produce a standard that is future-proof. All previous versions of the standard did prescribe a particular technology and method that must be used on all applicable cyber assets, and while that had no vagueness it became a huge burden on the industry for TFE's, putting the industry's focus on what could not be done rather than what could be done. Therefore, the SDT is leaving this requirement at a very high level that is in essence "think through the problem of malicious code introduction, detection, and prevention and come up with the best methods to handle the problem in each particular situation, and then document and do those methods." The SDT believes reliability will be better served in the long run by a requirement like this for such areas as the malicious code 'arms race' environment that we find ourselves in.

There were multiple comments asking if the 'or' is appropriate. There was another question if an awareness campaign to deter is ok. There was a suggested that the word 'deter' should be stricken. In response, the SDT notes that the

requirement was worded with the 'or' and 'deter' to avoid zero-defect language. If the requirement was to detect or prevent all malicious code, then despite an entity's best efforts if some zero-day malware did make it onto an applicable cyber asset the entity would be in violation of the requirement. As malware detection and prevention is an inexact science and essentially an 'arms race', the SDT did not want to word the requirement in such a way that it required perfection in an imperfect environment with imperfect tools.

There was many comments that the 'Associated PCAs' are included at a Cyber Asset (device) level, not a system level and should be deleted or clarified how the 'system' concept will apply. In response, the SDT notes that malware prevention really is at a Cyber Asset level and recognizes that the associated PCA's could be included by reference in the documentation the entity supplies for Requirement R3.1.

One commented stated Requirement R3.1 and R3.2 should be revised to "deploy methods … within an ESP" to scope to routable assets within the ESP. In response, the SDT notes that ESP's are only required around routable protocol connected cyber assets, however malware protection is required on all cyber assets in scope. Malware is a risk even on isolated systems; it may not be able to easily spread in non-routable environments, but it can be coded to have a specific impact even on isolated systems (e.g. Stuxnet was coded to do its harm when it reached a specific system and could travel by USB portable media). Therefore the SDT has chosen to not limit the malware prevention requirement to only routable protocol accessible systems in ESPs.

One commenter suggested that the measures should be revised to, "Entity's performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.)." In response, the SDT notes the only suggested change is the phrase 'non-software' in front of 'policies'. The SDT does not wish to make the measure more prescriptive than the requirement itself. Since malware prevention is an ever changing 'arms race' type environment where the controls needed are changing as the threat constantly evolves, the SDT is leaving this requirement at a high level. This will allow entities to adapt as the threat adapts while also reducing the need for TFEs.

One commenter stated that the last sentence of the guidance says 'should not require a TFE' making it unclear whether TFEs are an option or not. In response, the SDT agrees and has struck the phrase.

Requirement Part 3.2

One commenter recommended that the following sentence be added: “Mitigation for the Associated Protected Assets may be accomplished through other applicable systems.” In response, the SDT agrees that this is possible and the entity could state how the mitigation covers the associated PCA’s in their documentation for this requirement.

One commenter suggested that the wording “within 35 days” should be added as malware mitigation timeframe. In response, the SDT has chosen not to include a mitigation timeframe as in some cases the entity may be working with government or law enforcement in an ongoing investigation. In APT cases, quick mitigation may just force the moving of the attack while investigations are ongoing. The SDT feels that a mandatory timeframe would interfere with investigations in cases such as these.

Two commenters recommended that the measures should be limited to response actions for detected malware and remove other bullets. In response the SDT agrees and has removed the example measures that were more focused on specific technologies.

One commenter stated that in the guidelines it discusses ‘non-changeable software’ and asks if this is in conflict with definition of Cyber Asset. In response, the SDT believes it is not in conflict. Cyber Asset is a programmable electronic device and devices that are not updateable by the user, but are software or firmware based and do execute a program would still be classified as Cyber Assets.

Requirement Part 3.3

There were many comments that Medium impact locations with no remote connectivity need more than 35 days for signature updates or should not be in scope. Some commented that 35 days is too long for malware updates and it should be shortened. In response, the SDT agrees with both positions and realizes that specifying a time frame on a requirement such as this often means picking a timeframe that is usually not long enough for all of the more extreme cases while at the same time is too long for most ‘normal’ cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order 706 did not direct such a modification and the SDT is more concerned about preventing the unintended consequences of this timeframe and their resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade’s worth of viruses because they may not be able to get last month’s signatures on in 35 days. The SDT believes its in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an ‘arbitrary’ timeframe that satisfies no one.

One commenter stated that 35 days is too long for malware updates and should be shortened. In response, the SDT agrees with both positions and realizes that specifying a timeframe on a requirement such as this often means picking a timeframe that is usually not long enough for all the more extreme cases while at the same time is too long for most 'normal' cases. The SDT has decided that it is in the best interest of reliability to revert this requirement back to its V1-V4 language that did not include a timeframe. Order No. 706 did not direct such a modification and the SDT is more concerned with the unintended consequences of this timeframe and the resulting impacts to reliability. As one example, the SDT does not want to incent entities to remove antivirus products from systems in the field and expose them to a decade's worth of viruses because they may not be able to get last month's signatures on in 35 days. The SDT believes it is in the best interest of reliability to allow entities to put antivirus software on all assets where they can and require processes to test and install the updates without specifying an 'arbitrary' timeframe that satisfies no one.

Several commenters wrote that the requirement is not as clear as the change rationale and the requirement could be gamed to not install any recent sigs. In response, the SDT agrees and has rewritten the requirement for clarity.

A few comments stated that signature updates need to be staged to avoid a large impact of false positives. The included guidance should address this as well. In response, the SDT agrees and has reverted the language back to its V1-V4 state that did include a process for testing and installing the signature updates.

Some commenters questioned that if an entity does not use signature based tools, if they still have a process to update the signatures per the overall requirement. In response, the SDT notes the specific sub requirement is conditional and only applies to "for those methods identified in requirement part 3.1 that use signatures or patterns…" and therefore if an entity has no such methods, the requirement does not apply.

One commenter recommended that the word "available" should be changed to "applicable". In response, the SDT has rewritten the requirement for clarity and to address this and several other comments.

A commenter suggested that the requirement should allow for other anomaly or heuristics based analysis/detection, not just signature updates. In response, Requirement R3.1 allows for any method to be used so that the requirement does not preclude the use of any technology or tool as they constantly improve to keep up with the threats. Requirement R3.3 in particular is only applicable when an entity chooses to use a signature or pattern based tool in order to keep them updated in a timely manner; it does not require their use.

One commenter asked for clarity on what TFEs are allowed for equipment that doesn't run malicious code tools. In response, the SDT notes the requirement has been written at a much higher level than previous versions. The included guidance has numerous suggested methods up to and including policy level measures. Therefore, the SDT feels that TFEs are no longer an issue as the requirement no longer prescriptively requires a single technology tool for addressing the issue.

Requirement R4 General Comments

There were several comments that the rationale language should change 'immediate' detection to 'real time detection' to be consistent with 4.2. In response, the SDT received numerous comments that pointed out issues with the term 'real time' and has deleted it, as well as removing 'immediate' in the rationale.

There was a comment seeking clarity as to whether log events are required for local, remote, or both types of access. In response, the SDT notes that the requirement applies to both High and Medium impact BES Cyber Systems as well as all associated EACMs. The EACMs will include the EAPs for the associated perimeters. Therefore the logging is for both; local access at the BES Cyber Systems themselves, and remote access through the EAP.

One commenter suggested that the guidance include NIST 800-137 as a resource. In response, the SDT agrees and has added the reference to the guidance.

Requirement Part 4.1

Many commenters recommended that the requirement should add the phrase "per device capability". In response, the SDT agrees and has added this concept to the language.

Numerous commenters asked that it be clarified that devices that cannot log do not require a TFE. In response, the SDT has added device capability condition statements to the requirement such that the requirement does not apply if the device does not log the events. In addition, the bulleted list of logged events includes the qualifier 'detected' so that if a device cannot detect such events, then there is nothing to log.

There were several suggestions that 'where technically feasible' should be added to all. In response, the SDT's intent is that the requirement is worded so that what is required matches the device's capability and no more and avoids the use of TFE's due to prescriptive requirements that assume technical capabilities of large classes of Cyber Assets.

Tucson, and SME List commented that TFE should be applied to the logging, not the alerting in 4.2 and suggest removing the TFE in 4.2. In response, the SDT has changed both 4.1 and 4.2 to include the 'per device capability' concept rather than allowing TFE's.

Multiple commenters suggested said that the applicability should change to Medium Impact with ERC. In response, the SDT notes that logging should be enabled wherever it is available. If an isolated or standalone BES Cyber Asset is compromised, then the logs on that device may be the only data the entity will have to investigate the incident.

One commenter suggested that the measures should include samples of logs showing the events are being logged. In response, the SDT agrees and has added the additional example measure.

One commenter suggested that the requirement implies 100% availability of the logging system and suggests adding the 99.9% availability. In response, the SDT notes the comments where the 99.9% was added in CIP-006 pointed out numerous issues with that approach. The SDT believes that the inclusion of Requirement R4.3 states that 100% availability is not required and handles the issue by requiring the entity to have processes in place to respond to outages in a timely manner.

Several commenters sought clarity as to log failed access attempts when deny by default means offending packets are dropped such that there is nothing to log. In response, the SDT notes that a denied access attempt is a failed access attempt.

There were several commenters who suggested that 'malicious software' should be changed to 'malicious code' to be consistent with Requirement R3. In response, the SDT agrees and has made the change.

Many commenters recommended dropping the requirement since its determined after the fact, requires knowledge of intent, and it's not possible to produce a log of 'malicious activity'. In response, the SDT agrees and has removed the sub requirement.

Several commented stated that 4.1.4 is too vague and needs more guidance as to what activities beyond 4.1.1 to 4.1.3 would be included. In response, the SDT agrees and has removed the sub requirement.

One commenter stated that malicious activity should be detected and logged 'as required in the cyber security incident response plan'. In response, the SDT notes that based on several other industry comments, this sub requirement has been removed.

Requirement Part 4.2

Several commenter stated that 'real time' is not the appropriate phrase and some suggested changing to "Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary." In response, the SDT agrees and has deleted the 'real time' phrase.

Also, others commented that 'real time' should change to 15 minutes and add 'where the BES Cyber System is capable.' In response, the SDT agrees and has deleted the 'real time' phrase and the 'per Cyber Asset or BES System capability' has been added.

A few commenters recommended that 'within the BCS capabilities' be added. In response, the SDT agrees and has added the appropriate phrase.

One commenter stated that a minimum expected set of security events for which alerts should be issued should be prescribed (if the Cyber Asset is capable of detecting and logging those types of events). Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. They also commented that the guidance includes alerts to a display that may not be monitored. In response, the SDT notes that detected malicious code is included, as is detected event logging failure. The SDT agrees that unsuccessful login attempt threshold should be added as it is a requirement in CIP-007 R5.7 and has made this addition. The SDT notes that account lockout is a subset (or post action) of unsuccessful login attempt threshold and has not included it.

There was a comment that the requirement should only apply to Associated Protected Cyber Assets with ERC. In response, the SDT believes that if the BES Cyber Systems have External Routable Connectivity that the associated PCAs will also have that connectivity. In the envisioned rare instance where this is not the case, the requirement allows for the entity to do what is within the device's capability and no more.

One respondent commented that we need a requirement that trained and knowledgeable people perform the event monitoring activity. In response, the SDT agrees that this is certainly reasonable, but disagrees that it should be an

auditable requirement as it raises too many audit issues, such as what do the terms 'trained' and 'knowledgeable' mean and what is sufficient for each?

A commenter questioned is an alert required for malicious activity if it is automatically quarantined? In response, the SDT notes that alerts are required for detection of malicious code regardless of any subsequent mitigation actions taken. The SDT believes that if malicious code gets through the layers of defense and makes it way on to a BES Cyber System, that is an event that needs the entity's timely attention and response so the defenses can be shored up for the zero-day that is not detected and quarantined.

One commenter wrote that it was unclear as to whether 'detected failure' refers to logging a failure of some event or failure of logging. In response, the SDT has added a clarification that it is failure of the requirement part 4.1 event logging. This would include the failure of the applicable systems logging capability.

There was a recommendation that the measures should include examples of alerts issued. In response, the SDT agrees and has added this as one of the example measures.

Multiple comments suggested that 4.2.1 should change to 'detected cyber security event' since not all events are necessarily malicious. In response, the SDT agrees and has changed this part to refer to detected malicious code rather than malicious activity.

There were numerous comments suggesting to change the wording in 4.2.1 to 'detected events per 4.1'. In response, the SDT agrees and has added the reference to 4.1 for clarity.

One commenter stated that the guidance implies that only technical means are allowed, but requirement does not preclude procedural controls. In response, the SDT notes that the requirement language is the ruling language and guidance is not auditable and is provided to provide further context or examples or assistance in how entities may want to approach meeting the requirement.

Requirement Part 4.3

There were a multitude of commenters who recommended that the requirement add the phrase "human detected event logging failure" to clarify when the clock starts. In response, the SDT agrees with the concept and has changed the

language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

One commenter suggested that 'after notification' should be added after 'next calendar day'. In response, the SDT agrees with the concept and has changed the language to require that the response timeframe begins with the alert of the failure. Therefore, the timeframe begins after something or someone has detected the failure and has generated an alert as in 4.2.

A few respondents commented that the requirement should be struck or change the verbiage to "Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan." In response, the SDT agrees and has struck the requirement.

A few commenters stated that the next calendar day is not enough time to rectify issues. In response, the SDT notes the timeframe is to 'activate' a response, not to resolve the issue. The SDT has chosen this in recognition that depending on what caused the failure, there may be widely varying timeframes to resolve the issue. Therefore, the requirement is for timely initiation of a response.

One commenter noted that the requirement presumes but does not prescribe a mechanism for monitoring for logging system failures. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenter responded that the timeframe is too short due to distances or other operational situations. There was also a suggestion is to include 'next business day'. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There was one comment that this should only apply to Cyber Assets with ERC. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

Several commenters recommended that outage handling should be standardized with CIP-006. In response, the SDT agrees and in response to numerous comments and in keeping with handling logging failures in a 'non-zero defect' way has struck the requirement. The requirement to alert on logging failures remains but the entity must determine how to assess and correct the issue.

There were several comments that the measure should change the word 'attestation' to 'documentation'. In response, the SDT agrees and has made the change.

One comment suggested that the measure should change 'events' to 'failures' to better align with the requirement. In response, the SDT agrees and has made the change.

Requirement Part 4.4

There was a comment that the requirement should change to "Retain BES Cyber System and BES Cyber Asset". In response, the SDT agrees with the concept that the applicability in the requirement did not match the applicability column and has removed the applicability from the requirement by replacing 'BES Cyber System' with 'applicable'.

There were several comments that the TFE language should be struck and add 'within the BCS capabilities." In response, the SDT notes that this requirement is scoped to Control Center environments where the highest degree of logging is required and has the highest degree of more capable Cyber Assets. The SDT feels that in this environment, the industry really should push for 90 days of log retention on these systems.

One commenter suggested that this should apply to all Medium's that can store logs, not just those at control centers. In response, the SDT notes that with the vastly increased numbers and types of field devices that Version 5 will bring into scope, most of which are legacy devices, that putting a mandatory requirement in place that prescribes the length of log retention is not warranted and would cause numerous TFE's.

One commenter wrote that 'identified in 4.1' should be the main qualification for log retention and delete the 'security related' portion for clarity. In response, the SDT agrees and has removed the phrasing.

Some commenters stated that this is in conflict with evidence retention section. Auditors expect to ask for any day's logs in past three years. In response, the SDT has added guidance around this topic. The requirement that is to be audited is

that applicable cyber assets maintain 90 days of logs. The compliance evidence requirement is that the entity be able to show that for the historical compliance period, the applicable cyber systems maintained 90 days of logs. The guidance speaks of records of disposition of logs after their 90 days is up.

BPA commented that a media hardware failure that results in loss of stored logs is still a violation. In response, the SDT agrees and has added "except under CIP Exceptional Circumstances" to the requirement as it includes hardware failure.

One commenter stated that this should allow for a timeframe as determined by the Responsible Entity. In response, the SDT notes that 90 days has been the precedent through the previous CIP versions and having no bound means that zero days is valid if determined by the entity. The SDT believes that 90 days is a sufficient lower bound for Control Center environments and has no justification for lowering it in the highest risk environments.

A commenter suggested that the applicability should apply to medium impact with ERC. In response, the SDT notes that this applies to Control Centers. Throughout the history of the CIP standards, all cyber assets in a Control Center are in scope regardless of external connectivity. The SDT believes there is insufficient justification to lower the standard on this point.

One commenter implied that measure 2 requests info about log data that is not in the requirement. Measures 1 and 3 cover the requirement. In response, the SDT agrees and has moved this to the guidance section with a more detailed explanation of the difference between the requirement's retention period for security purposes and the overall standard's requirement for compliance measurement purposes.

Requirement Part 4.5

Many responders commented that clarity around who determines the appropriate sampling should be added by including 'sampling as deemed appropriate by the Responsible Entity'. In response, the SDT agrees and has made the change.

Several commenters noted that the applicability should be 'High impact including associated PCA' to clarify logging reviews aren't at the device level and should exclude EACM/PACMs. In response, the SDT agrees and has modified the applicability, however EACMs should be included. Since Electronic Access Points to ESP's are EACMs, this is one of the primary logs that should be reviewed.

Several commenters expressed concern that this needs some minimum expectations for logged event review. In response, the SDT notes the intent is included in the requirement which is to identify undetected security incidents. The FERC Order in paragraphs 525 and 628 states, "However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Furthermore, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings. If a firewall setting is incorrect or ineffective, an automated review system may not identify a cyber security intrusion. For those entities without automated log review and alerts, it is even more important to perform a manual review because this will be the only review of the logs." The SDT believes the intent is that entities manually review logs to insure that automated tools are tuned and alerting on real incidents. The SDT does not believe it should get more prescriptive with the requirement.

There were several commenters who noted that the requirement should change to "Document and implement a secondary control(s), and an associated interval, not to exceed two weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1." In response, the SDT notes that the FERC Order 706 in paragraphs 525 and 628 are explicit about a manual review. Also, the events identified in 4.1 are requirements so identifying events in 4.5 that should have been caught in 4.1 is a violation. The intent is for the entity to review the logs to see if there are events happening (other than those in 4.1) that the entity should be alerting on. In essence, this is a 'tuning' requirement to insure that an entity's automated Security Information and Event Management (SIEM) type tools are not missing conditions that are appearing in the logs and going undetected.

One commenter suggested that the requirement should change 'undetected' to 'potential Cyber Security Incidents not previously identified or detected'. In response, the SDT notes that in draft one the language included terms such as "unanticipated" and "potential" and received numerous comments to remove these subjective terms.

There were a number of concerns that two weeks is too short and suggest monthly or two month periodicity. In response, the SDT notes that in paragraph 628 of FERC Order 706 states, "The Commission continues to believe that, in general, logs should be reviewed at least weekly", but leaves it to the ERO to determine the appropriate timeframe. The SDT believes that bi-weekly is an appropriate timeframe given the Commission's statement concerning weekly reviews.

There was a comment that the phrase “at a minimum every two weeks” could be misconstrued and suggested to mean “at intervals no greater than 15 days.” In response, the SDT agrees that two weeks is a maximum not a minimum and adopts the suggested change.

There was a suggestion in changing the requirement to read “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.” In response, the SDT agrees with the issue and has reworded the requirement based on this and other comments to utilize ‘intervals no greater than 15 days’ for greater specificity.

One commenter suggested that the timeframe should be determined by the Responsible Entity. In response, the SDT notes that in paragraph 628 of FERC Order 706 the Commission ordered the ERO to determine an appropriate timeframe that is less than the 90 days in the requirements of previous versions while stating that weekly reviews are their recommendation. The SDT sees no justification for how this directive can be met if the timeframe is left completely up to the entity to determine.

There were multiple suggestions that the applicability should only apply when automated processes and alerting are not possible or no managed service provider is utilized. In response, the SDT notes from paragraph 525 of FERC Order 706 that “the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings.” The Commission goes on to order the inclusion of manual review even if automated alerts are employed.

One commenter stated that a SIEM is the only real solution and is too expensive for small entities. In response, the SDT notes the requirement is for a manual review, not an automated review. Paragraph 525 of Order 706 makes it clear that even if automated systems are used, the manual review is still required. The requirement does not require installation of SIEM tools, but requires manual review even if SIEM tools are in use.

Several commenters noted that the phrase “signed and” should be deleted in the measure (also in 4.1 measure). In response, the SDT agrees that a signed approval of the review is not in the requirement and this has been deleted from the measure.

QUESTION B24– CIP-007-5 REQUIREMENT R5:

If you disagree with the changes made to CIP-007-5, Requirement R5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, some of the key issues expressed by commenters included (1) the applicability to Medium Impact BES Cyber Systems with external routable connectivity, particularly in requirement part 5.1 and (2) the obligation for the CIP Senior Manager to authorize specific account types for BES Cyber Systems. The consideration of comments according to major issues and standard sections follows.

Correcting Deficiencies

One comment stated that this requirement should have a find, fix, track, and report mechanism built in so that entities can fix administrative deficiencies rather than consider them a violation of the requirement. In response, the CIP Version 5 approach to correcting deficiencies is that each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in the specified table. This approach of correcting deficiencies complements the compliance concept of internal controls.

Applicability to Low Impact

One commenter suggested that CIP-007-5 R5 should apply to Low Impact BES Cyber Systems. In response, we note the challenge of applying device-specific mandatory and enforceable requirements to low impact BES Cyber Systems exists in the overwhelming number of BES Cyber Assets. NERC survey results from the 2011 CIP filing indicate 90% of the facilities would be considered low impact, and each of these sites can have a potentially large number of Cyber Assets. As a result, the SDT has taken the approach of applying policy level requirements to BES Cyber Systems with the understanding and expectation that the compliance audit and enforcement of the policies will adapt to the significant increase.

TFE for all Requirement Parts

One commenter suggested adding TFE language for the entire requirement due its technical nature. In response, the SDT has identified requirement parts that intentionally allow for a safe-harbor exception process where equivalent mitigation can be shown. However, in some cases, we do not intend the technical limitations of the device to indicate a violation or need for safe-harbor (e.g. password complexity).

Multifactor Authentication
One commenter questioned if multi-factor authentication can replace password authentication without a TFE. In response, the SDT notes that the said requirement applies to password-only authentication but do not preclude other strong authentication mechanisms.

Procedural Controls
One commenter suggested, with regard to CAN-0017, procedural controls should be explicitly allowed in the requirement. However, the SDT points out that Compliance Application Notices do not carry forward to new versions of the standard. Previous versions require both procedural and technical controls for passwords, but this language is not included in the current draft. It would cause more confusion to explicitly allow procedural controls for each requirement part.

Version 5
One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

Summary of Changes Section
Two commenters noted the summary of changes does not correspond to requirements for shared accounts, and in response the SDT has deleted this section which was held over from previous versions.

Requirement Part 5.1
Several entities commented this requirement part should be limited to medium impact with External Routable Connectivity, and the SDT has made this change. However, this requirement still applies to Medium Impact BES Cyber Systems at Control Centers.

Several commented that user access should be a defined term and security controls for system accounts should also exist. In response, we provide a definition in the guidelines, and we believe this term is well understood. In addition, the SDT has added a qualifier for this to apply to interactive user access. We do not define the same controls for system access due to the widely diverse way this could apply. System accounts do not uniformly apply across all devices and operating systems.

Several entities suggested rewording the phrase “where technically feasible” to “within the capability of the BES Cyber System”. In response, the alternative language would not change the TFE trigger for this requirement. There are several instances in which strict compliance can still be met in the absence of a specific technology mechanism to enforce access. The SDT has provided examples in the rationale box for requirement part 5.1 and improved the requirement language to make this point clear.

One commenter requested clarification that user access does not mean front panel read-outs on a device. In response, the SDT has changed “user access” to “interactive user access”, and the SDT has added a rationale statement further describing the intent of this requirement, in which the SDT has explicitly stated front panel read-outs do not qualify as interactive user access.

One commenter proposed that this requirement should be rephrased to limit to only electronic access. In response, the subject matter of the standard and requirement suffice to make the distinction, and we do not want to limit or confuse the possibility of using properly configured physical access controls to demonstrate compliance with this requirement.

One commenter suggested this apply to accounts and not user access. In response, the SDT has chosen to apply this to interactive user access because there may be instances where you do not want to enforce authentication for read-only access.

One commenter suggested specifying the phrase “applicable cyber assets” to qualify this requirement, but the applicability column already qualifies the requirement.

Requirement Part 5.2

Several entities suggested deleting requirement part 5.2 because it is already covered by the CIP-004-5 requirement to authorize users. In response, this requirement only deals with identifying the use of account types. It has been modified to make the intent clearer. Identifying the use of default or generic account types that could introduce vulnerabilities has the benefit ensuring entities understand the possible risk these accounts pose to the BES Cyber System. The requirement part avoids prescribing an action to address these accounts because the most effective solution is situation specific, and in some cases, removing or disabling the account could have reliability consequences.

Several commenters advised removing the CIP Senior Manager as the person authorizing these account types. In response, the SDT chose not to remove this in the previous posting as suggested by our previous response to comments, and the SDT has removed the CIP Senior Manager as the person authorizing the account types in this posting.

One commenter proposed that generic accounts must be specified. In response, the SDT has added examples in the guidance section of this standard. The section added reads: "Where possible, default and other generic accounts provided by a vendor should be removed, renamed, or disabled prior to production use of the Cyber Asset or BES Cyber System. If this is not possible, the passwords must be changed from the default provided by the vendor. Default and other generic accounts remaining enabled must be documented. For common configurations, this documentation can be performed at a BES Cyber System or more general level."

One commenter suggested removing the word "authorized" from this requirement. The SDT has incorporated this suggestion by replacing the word "authorized" with the phrase "identify and inventory".

There was a comment submitted as to whether this requirement restricts the use of the specified account types. In response, identification of the accounts provides the necessary control. We do not specify these accounts must be disabled or removed because they are sometimes necessary for operation. Restricting these based on least privilege or need to know is already covered in CIP-004-5 R6.

One commenter suggested that authorization by "delegate(s)" be substitute for "delegate". However, the SDT has removed the requirement to authorize by CIP Senior Manager based on other commenters.

Requirement Part 5.3

Several comments suggested deleting requirement part 5.3 because it is already covered in CIP-004-5 requirements to authorize access. However, the identification of individuals with access to shared account has the additional objective of mitigating the risk of unauthorized access through shared accounts. This differs from the CIP-004-5 Requirement R6 to authorize access. An entity can authorize access and still not know who has access to a shared account. This would make it difficult to revoke access when it is no longer needed.

Several suggested incorporating the change rationale stating that the phrase "individuals storing, losing or inappropriately sharing a password is not a violation of this requirement." In response, the SDT has added this language to the rationale box for CIP-007-5 R5. The language in this section reads, "The term "authorized" is used in the

requirement to make clear that an individual storing, losing or inappropriately sharing a password is not a violation of this requirement."

Multiple commenters suggested adding the word "authorized" as a qualifier for access to correspond to the requirement language, and the SDT has made this change.

One commenter suggested that this requirement does not go far enough to restrict the use of privileged access, particularly when operating software. In response, CIP-004-5 R6 restricts the use of privileged access to only those having a documented business need. We do not specify the individual use of privileged and non-privileged access because this is not auditable for mandatory enforceable requirements. This is a good practice, but if this practice were codified in a standard, any individual not following the policy would impose monetary penalties on an organization.

One commenter suggested that the external routable connectivity qualifier should be removed for this Requirement Part in the applicability to match requirement part 5.2. In response, the requirement parts are unrelated, and the qualifier matches that of CIP-004-5 R6, which requires the authorization for electronic access.

Requirement Part 5.4

Several comments suggested revising this requirement part to address a recent RuggedCom vulnerability where a default password was unique to publicly known attributes of the device. In response, the SDT has removed the requirement exception where the "default password is unique to the device or instance of the application", and specified in the rationale that "pseudo-randomly system generated passwords are not considered default passwords".

Several commenters suggested adding the word "known" as a qualifier to default password to avoid the case where the entity was not aware of an undocumented default password by the vendor. The SDT has made this change.

There were several comments that the measure should change the phrase "new devices are deployed" to "new devices are in production" and one commenter suggested removing the phrase altogether since timeframes are covered in the implementation plan. The SDT has made this change from the word "deployed" to "in production", but the timeframe here does not conflict with the implementation timeframe and provides example, high quality evidence to meet this requirement.

One commenter requested clarification of when the default password should be changed. In response, we do not specify a timeframe (i.e. when cyber assets go into production) which could be misinterpreted. Instead, as with all requirements of CIP-007-5, this requirement must be met when a device becomes one of the applicable systems or assets.

Several commenters suggested removing the term "Cyber Assets" within the requirement to match the applicability of BES Cyber System. In response, the SDT has removed this language in deference to the applicability column.

One commenter requested clarification that default password that are unchanged would require changing according to R5.6. In response, this may be the case for interactive user accounts, but this is not necessary to state in the requirement. Changing default passwords meets a different objective to prevent unauthorized access from known credentials.

One commenter suggested excepting when a password is unique to the device. However, many commenters point out that doing so would allow for vulnerabilities where the uniqueness of the device where publicly known (i.e. MAC address).

Requirement Part 5.5

Several commenters suggested modifying the measure for requirement part 5.5 and requirement part 5.6 to better describe the attestation. Another commenter suggested replacing attestations with the ability to present a procedure. Others noted that it is not possible to obtain attestation from unionized workers and suggested adding a separate requirement to use training as a procedural control in place of attestations. In response, the SDT has used provided language to better describe the attestation evidence. The suggestion to use presentation of a procedure as a replacement cannot be used as evidence of implementing a procedure. The suggestion to have a further requirement for training is already covered in the training program specified in CIP-004-5.

One commenter stated that password complexity should be enforced to the maximum extent technically possible. In response, the SDT noted such a policy would create situations where users must write down passwords to remember them. The maximum extent could be exorbitant in some cases.

One commenter also stated that the guidelines state this requirement part is for password-only authentication, but the requirement does not include the same stipulation. BPA and Salt River Project made similar comments to distinguish the case where a PIN is used for multi-factor authentication. In response, the SDT has changed "password-based" to "password-only" in both requirement part 5.5 and 5.6.

Several commenters suggested using verbiage for requirement part 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” In response, although the proposed verbiage is cleaner, it becomes less clear once we specify “system” and the number of characters in the proposal. The SDT therefore decided to continue with the currently drafted language.

One commenter questioned if this new requirement will remove CAN-0017. In response, CANs do not apply to future versions of the standard, and the SDT has explicitly addressed the issue raised by CAN-0017 that either technical or procedural mechanisms can meet the requirement.

One commenter stated that it does not agree with the proscription of password requirements. In response, the SDT has included more prescriptive password requirements in response to a large number of industry comments against having added flexibility. However, the SDT has also attempted to remove some of the problematic provisions of the current version of password requirements that would allow entities to have stronger password policies.

One commenter suggested that the password complexity in requirement part 5.5.2 should specify or define the word “type”. In response, the examples provided in the requirement suffice for specifying password character types. The SDT believes these terms are well-understood by industry and do not necessitate further definitions.

Requirement Part 5.6

Several commenters pointed out the guidance, particularly the recommended password length table, has not updated to reflect the requirement. In response, the SDT has deleted sections of the guidance which no longer have relevance to the requirement.

Several commenters suggested adding a technical feasibility clause to this requirement part because some devices do not allow this capability. In response, the SDT notes that this only applies to user access, and the SDT has modified the requirement part to clarify this. The language as the end of this requirement part reads, “…at least once each calendar year, not to exceed 15 calendar months between changes, where technically feasible.”

One commenter suggested this requirement part explicitly apply to interactive user access, and the SDT has modified this requirement part to address the concern. The beginning of this requirement part reads, “For password-only authentication for interactive user access, either technically or procedurally enforce password changes…”

One commenter suggested adding the language “unless it impacts operation of the BES” to this requirement part. In response, the SDT has added the phrase “where technically feasible” to address these type of exceptions.

One commenter suggested the applicability of 5.6 be modified to match other requirement parts in CIP-007-5 R5. In response, the applicability to those Medium Impact BES Cyber Systems with External Routable Connectivity is due to the periodic nature of this requirement, which may only be feasible on large systems by having such connectivity. The commenter also suggested periodically is misspelled periodicity, but the SDT intends the latter as this is an attribute of the policy instead of a modifier.

One commenter suggested incorporating the language in the guidance table to include periodicity provisions for plant outages and disabled accounts. In response, for disabled accounts, a password change is not required because these do not qualify as providing interactive user authentication. The requirement does not have provisions for plant outages due to the widely varying schedules for plant outages. The SDT also notes that this requirement applies to those Medium Impact BES Cyber Systems with External Routable Connectivity.

A commenter proposed having a password change every 15 months. The SDT has incorporated this suggestion as part of an overall modification of annual periodic requirements in the CIP standards.

A commenter proposed to allow the entity to specify a password change periodicity, but the SDT has specified this periodicity based on a large number of comments against having this flexibility.

There was one comment that suggested the password change periodicity should be much shorter (i.e. quarterly). In response, the SDT notes that password change requirements should be considered in context with all of the password requirements, and shorter password change requirements can often result in poor password protection and selection by individuals.

Requirement Part 5.7

Several commenters suggested this requirement has the potential for creating a denial of service vulnerability to lockout all accounts to the system if entities configure all accounts for lockout. The SDT has not included the proposal to specify “user accounts” for limiting login attempts because it is too specific and has the potential to cause confusion. Although

the requirement does not prescribe this vulnerability, it does allow for it. Consequently, the SDT has included guidance in avoiding this configuration in the rationale.

Several commenters requested clarification on what the clause "where technically feasible" qualifies for this requirement part. In response, this requirement part has been modified to make clear the TFE triggering language qualifies both options. Furthermore, a TFE would only be necessary based on failure to implement either option.

Several commenters suggested this requirement should be deleted as it was not directed by FERC or otherwise align with the alerting requirements of CIP-007-5 requirement part 4.2. In response, this requirement is part of a more reasonable overall password security standard. As a trade-off to providing more flexibility to password policies, this requirement is highly effective to prevent online password attacks. This does not duplicate CIP-007-5 requirement part 4.2 because this alert is not required to be configured by that requirement.

One commenter requested additional guidance on the threshold for unsuccessful login attempts. The SDT has added this to the guidance section of this standard. Language was added which reads, "The threshold of failed authentication attempts should be set high enough to avoid false-positives from authorized users failing to authenticate."

Multiple commenters suggested that a minimum threshold parameter for account lockout should be specified. In response, a value is not specified here because this requirement protects against password cracking through online password cracking. Given the additional password policy requirements, the threshold for this setting can be very high, up to 100 or more.

One commenter requested the requirement part make clear these do not apply to Protected Cyber Assets such as printers and multi-function machines. In response, this requirement does apply to Protected Cyber Assets. This is a part of an overall protection against unauthorized access, which would include Protected Cyber Assets that have direct connections with the BES Cyber System.

VRFs

There was one comment that suggested the VRF should be Lower for Medium Impact BES Cyber Systems. In response, the impact level of the BES Cyber System is accounted for by the applicability of CIP-004 through CIP-011 requirements. A violation for a Medium Impact BES Cyber System cannot be considered directly with a High Impact BES Cyber System because they have less application of compensating security requirements.

VSLs

There was one comment that noted the High VSL includes the phrase “use of” where the associated requirement refers to only enablement of generic accounts and that the Severe VSL includes criteria for failure to implement password procedures, which might imply the required use of passwords. The VSL language regarding the enablement of generic account types has been updated to match the requirement. We do not agree the Severe VSL language implies a requirement to only use passwords. The VSLs are only used to describe violations, and use of authentication alternatives to passwords would not be a violation.

One commenter noted the Severe VSL is not consistent with the requirement and the SDT has updated the VSLs to align with modifications to the requirement.

Guideline

There was a recommendation that the guideline section needs to define generic accounts, and the SDT has added this to the guidelines.

Questions with Votes Only:

CIP-004, CIP-005, CIP-006 and CIP-007 Questions:

1. CIP-004-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
NESCOR/NESCO	No
ACES Power Marketing	No
Hydro One	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No

Organization	Yes or No
NextEra Energy, Inc.	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Springfield Utility Board	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes

Organization	Yes or No
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes

Organization	Yes or No
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
PJM Interconnection	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes

Organization	Yes or No
Utility Services Inc	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

2. CIP-004-5 R2 states "Each Responsible Entity shall have a role-based cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No

Organization	Yes or No
LCEC	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Snohomish County PUD	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
San Diego Gas & Electric	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177,	Yes

Organization	Yes or No
JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes

Organization	Yes or No
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

3. CIP-004-5 R3 states "Each Responsible Entity shall implement its documented role-based cyber security training program to attain and retain authorized electronic or unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R3 - Cyber Security Training." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No
IRC Standards Review Committee	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
NRG Energy Companies	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

4. CIP-004-5 R4 states "Each Responsible Entity shall have one or more documented personnel risk assessment programs to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively includes each of the applicable items in CIP-004-5 Table R4 – Personnel Risk Assessment Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No
ACES Power Marketing	No
IRC Standards Review	No

Organization	Yes or No
Committee	
CenterPoint Energy	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No

Organization	Yes or No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
New York Power Authority	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
NCEMC	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Arizona Public Service Company	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes
California ISO	Yes

5. CIP-004-5 R5 states "Each Responsible Entity shall implement one or more documented processes to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable elements in CIP-004-5 Table R5 – Personnel Risk Assessment." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
LCEC	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
PSEG	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
Duke Energy	Yes
PNGC Comment Group	Yes
Dominion	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes

Organization	Yes or No
SPP and Member companies	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
PNM Resources	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity	Yes

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

6. CIP-004-5 R6 states "Each Responsible Entity shall implement one or more documented access management programs that collectively include each of the applicable elements in CIP-004-5 Table R6 – Access Management Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R6?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Pepco Holdings Inc & Affiliates	No
SMUD & BANC	No

Organization	Yes or No
PNM Resources	No
CIP Version 5 Comment SME list	No
Southern Company Services, Inc.	No
Southern California Edison company	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Ameren	No

Organization	Yes or No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
NYISO	No
Farmington Electric Utility System	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
Arizona Public Service	Yes

Organization	Yes or No
Company	
Western Area Power Administration	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
ISO New England Inc.	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

7. CIP-004-5 R7 states "Each Responsible Entity shall implement one or more documented access revocation programs that collectively include each of the applicable items in CIP-004-5 Table R7 – Access Revocation." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R7?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Colorado Springs Utilities	No

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
SPP and Member companies	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service Company	No
Southern Company Services, Inc.	No
Southern California Edison company	No

Organization	Yes or No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
ATCO Electric	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Lakeland Electric	No
Ameren	No
NextEra Energy, Inc.	No
Northeast Utilities	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
MEAG Power	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Springfield Utility Board	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services	Yes

Organization	Yes or No
Corporation	
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Liberty Electric Power LLC	Yes
PSEG	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes

Organization	Yes or No
Cowlitz County PUD	Yes

10. CIP-005-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1 – Electronic Security Perimeter." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
ACES Power Marketing	No

Organization	Yes or No
SPP and Member companies	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy	No

Organization	Yes or No
Company	
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California ISO	No

Organization	Yes or No
NRG Energy Companies	Yes
FirstEnergy	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes

Organization	Yes or No
NIPSCO	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of	Yes

Organization	Yes or No
Water and Power	
US Bureau of Reclamation	Yes

11. CIP-005-5 R2 states "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
PPL Corporation NERC Registered Affiliates	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
ACES Power Marketing	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Progress Energy	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No

Organization	Yes or No
PSEG	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba	Yes

Organization	Yes or No
National Grid)	
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
NIPSCO	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
US Bureau of Reclamation	Yes

14. CIP-006-5 R1 states "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards	No

Organization	Yes or No
Review Subcommittee	
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
Puget Sound Energy, Inc.	No
PNM Resources	No
BC Hydro	No
Hydro One	No
CIP Version 5 Comment SME list	No
Arizona Public Service	No

Organization	Yes or No
Company	
Southern Company Services, Inc.	No
Western Area Power Administration	No
Salt River Project	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No

Organization	Yes or No
Lincoln Electric System	No
United illuminating Company	No
Xcel Energy	No
NV Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Northeast Utilities	No
PSEG	No

Organization	Yes or No
San Diego Gas & Electric	No
Texas Reliability Entity	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
MEAG Power	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Los Angeles Department of Water and Power	No
Brazos Electric Power Cooperative	No
US Bureau of Reclamation	No
Kansas City Power & Light	No
California ISO	No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
Tri-State G&T - Transmission	Yes

Organization	Yes or No
Southern California Edison company	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
The Empire District Electric Company	Yes
Utility Services Inc	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

15. CIP-006-5 R2 states "Each Responsible Entity shall implement one or more documented visitor control programs that include each of the applicable items in CIP-006-5 Table R2 – Visitor Control Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Duke Energy	No
Dominion	No
Florida Municipal Power Agency	No
PNM Resources	No
BC Hydro	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity	No

Organization	Yes or No
System Operator	
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
Portland General Electric	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its	No

Organization	Yes or No
affiliates	
Deseret Power	No
Los Angeles Department of Water and Power	No
California ISO	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
FirstEnergy	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC)	Yes

Organization	Yes or No
including OPC, GTC & GSOC	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Snohomish County PUD	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes

16. CIP-006-5 R3 states "Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
IRC Standards Review Committee	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
Western Area Power Administration	No
Progress Energy	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Xcel Energy	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
NextEra Energy, Inc.	No

Organization	Yes or No
Texas Reliability Entity	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
New York Power Authority	No
Los Angeles Department of Water and Power	No
PPL Corporation NERC Registered Affiliates	Yes
Duke Energy	Yes
Dominion	Yes
FirstEnergy	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison company	Yes
Dairyland Power Cooperative	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security	Yes

Organization	Yes or No
Technologies, Inc.	
Utility Services Inc	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

Organization	Yes or No
Kansas City Power & Light	Yes
California ISO	Yes

18. CIP-007-5 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R1 – Ports and Services." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Summary Consideration:

Organization	Yes or No
PPL Corporation NERC Registered Affiliates	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Florida Municipal Power Agency	No
SMUD & BANC	No

Organization	Yes or No
CenterPoint Energy	No
PNM Resources	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
LCEC	No
Consumers Energy Company	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Lakeland Electric	No
NextEra Energy, Inc.	No
PJM Interconnection	No
Wisconsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
Exelon Corporation and its affiliates	No
Kansas City Power & Light	No
California ISO	No
Northeast Power Coordinating Council	Yes
PNGC Comment Group	Yes
FirstEnergy	Yes
MRO NSRF	Yes

Organization	Yes or No
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
Colorado Springs Utilities	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Hydro One	Yes
CIP Version 5 Comment SME list	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes

Organization	Yes or No
Snohomish County PUD	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
Oncor Electric Delivery Company LLC	Yes
NIPSCO	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Alliant Energy	Yes
New York Power Authority	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

19. CIP-007-5 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R2 – Security Patch Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No

Organization	Yes or No
Hydro One	No
Arizona Public Service Company	No
Western Area Power Administration	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Hydro-Quebec TransEnergie	No
LCEC	No
Lincoln Electric System	No
Xcel Energy	No
Bonneville Power Administration	No
Tampa Electric Company	No
MidAmerican Energy Company	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Kansas City Power & Light	No
PPL Corporation NERC Registered Affiliates	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power	Yes

Organization	Yes or No
Agency	
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes

Organization	Yes or No
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power	Yes

Organization	Yes or No
Cooperative	
US Bureau of Reclamation	Yes
California ISO	Yes

20. CIP-007-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R3 – Malicious Code Prevention." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SPP and Member companies	No
CenterPoint Energy	No

Organization	Yes or No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Bonneville Power Administration	No
Snohomish County PUD	No
MidAmerican Energy Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No

Organization	Yes or No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
NRG Energy Companies	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes

Organization	Yes or No
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Western Area Power Administration	Yes
Salt River Project	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCEC	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
The Empire District Electric Company	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes

Organization	Yes or No
NIPSCO	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Tucson Electric Power	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes

Organization	Yes or No
US Bureau of Reclamation	Yes

21. CIP-007-5 R4 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R4 – Security Event Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R4?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
SPP and Member companies	No
IRC Standards Review Committee	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
CIP Version 5 Comment SME list	No
Western Area Power Administration	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No

Organization	Yes or No
Hydro-Quebec TransEnergie	No
Lower Colorado River Authority	No
LCEC	No
LCRA Transmission Services Corporation	No
Niagara Mohawk (dba National Grid)	No
National Grid	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No
NIPSCO	No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No
Network & Security Technologies, Inc.	No
Utility Services Inc	No

Organization	Yes or No
Alliant Energy	No
New York Power Authority	No
Pacific Gas and Electric Company	No
NYISO	No
Tucson Electric Power	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Dominion	Yes
Associated Electric Cooperative, Inc (NCR01177, JRO00088)	Yes
Colorado Springs Utilities	Yes

Organization	Yes or No
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Clallam County PUD No.1	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
United illuminating Company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Liberty Electric Power LLC	Yes
Northeast Utilities	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

22. CIP-007-5 R5 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-007-5 Table R5 – System Access Controls." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R5?

Summary Consideration:

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Duke Energy	No
Dominion	No
NESCOR/NESCO	No
FirstEnergy	No
MRO NSRF	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
SMUD & BANC	No
CenterPoint Energy	No
PNM Resources	No
Hydro One	No
Southern Company Services, Inc.	No
Salt River Project	No
Southern California Edison company	No
Progress Energy	No
Dairyland Power Cooperative	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Consumers Energy Company	No

Organization	Yes or No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
Lakeland Electric	No
Tennessee Valley Authority	No
Ameren	No
Liberty Electric Power LLC	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
Oncor Electric Delivery Company LLC	No
PJM Interconnection	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Wisconsin Electric Power Company	No
ISO New England Inc.	No
Portland General Electric	No
City Utilities of Springfield, MO	No
Alliant Energy	No
New York Power Authority	No
NYISO	No
Tucson Electric Power	No
Kansas City Power & Light	No
California ISO	No
PPL Corporation NERC Registered Affiliates	Yes
PNGC Comment Group	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc (NCR01177, JRO00088)	
Colorado Springs Utilities	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Tri-State G&T - Transmission	Yes
Puget Sound Energy, Inc.	Yes
BC Hydro	Yes
CIP Version 5 Comment SME list	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Clallam County PUD No.1	Yes
Hydro-Quebec TransEnergie	Yes
ATCO Electric	Yes
LCEC	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
NV Energy	Yes
The Empire District Electric Company	Yes
Northeast Utilities	Yes
PSEG	Yes

Organization	Yes or No
Texas Reliability Entity	Yes
NIPSCO	Yes
MEAG Power	Yes
Network & Security Technologies, Inc.	Yes
Utility Services Inc	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

Organization	Yes or No
Brazos Electric Power Cooperative	Yes
US Bureau of Reclamation	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form C
CIP-008 through CIP-011

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 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.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
7.	Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8.	Annie Terracciano	Northern Lights Inc.	WECC 3										
9.	Aleka Scott	PNGC	WECC 4										
10.	Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12.	Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13.	Margaret Ryan	PNGC	WECC 8										
12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14.	Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	M & A Electric Power Cooperative		SERC	1, 3
4.	Northeast Missouri Electric Power Cooperative		SERC	1, 3
5.	N.W. Electric Power Cooperative, Inc.		SERC	1, 3
6.	Sho-Me Power Electric Cooperative		SERC	1, 3

15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Oglethorpe Power Corporation		SERC	5
2.	Georgia Transmission Corporation		SERC	1

16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWERENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
8.	SCOTT NICKELS	RPU	MRO	4
9.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
10.	MARIE KNOX	MISO	MRO	2
11.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
12.	SCOTT BOS	MPW	MRO	6, 1, 3, 5
13.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
14.	THERESA ALLARD	MPC	MRO	1, 3, 5, 6

17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	James Howard	Lakeland Electric	FRCC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Darl Shimko	MGE	MRO	3
2.	Joseph DePoorter	MGE	MRO	4
3.	Steve Schultz	MGE	MRO	5
4.	Jeff Keebler	MGE	MRO	6

20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Jones	Pepco	RFC	1

21.	Group	Rick Terrill	Luminant					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6
9.	Brenda Hampton	Luminant Energy Company LLC		

22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Smith	BANC	WECC	1

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION C4 – CIP-008-5:

If you disagree with the changes made to CIP-008-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, most of the comments resulted in changes that improved clarity and did not require significant structural revisions. The consideration of comments according to major issues and standard sections follows.

References to EOP-004-2
The comments received for CIP-008-5 and EOP-004-2 both indicated support for handling the reporting of Cyber Security Incidents in CIP-008-5. EOP-004-2 received a much lower ballot approval in its most recent posting primarily for the one hour timeframe required for reporting Cyber Security Incidents. The commenters concern for EOP-004-2 was the lack of a timeframe for identifying a Cyber Security Incident. The required CIP-008-5 processes make clear that reporting to the ES-ISAC occurs within one hour of the analysis to determine whether an event would constitute a Cyber Security Incident. As a result, both drafting teams agreed to move the Cyber Security Incident reporting to the ES-ISAC to CIP-008-5. However, the SDT wishes to stress the reporting threshold is not necessarily one hour from the Cyber Security Incident occurrence. Instead, the threshold accounts for the analysis that must be performed in identifying the Cyber Security Incident. The incident could even have occurred much earlier without any observable behavior. Also, entities can still have a single reporting process to comply with the new versions of EOP-004 and CIP-008.

Applicability Section
Several commented that all instances of Medium Impact BES Cyber Systems should be changed to "Medium Impact BES Cyber Systems with External Routable Connectivity". In response, we note that CIP-008-5 addresses incident response and reporting and the lack of external routable connectivity would not address this issue. It is possible for a Cyber Security Incident to occur on such cyber systems through insider attacks or other means of penetrating the physical or electronic boundaries. This does not create an inconsistency among the standards or implied requirement for monitoring because an entity can have a monitoring program to detect incidents that does not fully meet the requirements of CIP-006-5 and CIP-007-5.

There were several comments that stated CIP-008-5 should apply to Electronic Access Control and Monitoring Systems and Physical Access Control Systems. In response, applicability to these systems is unnecessary because the incident is associated to the BES Cyber Systems. Incidents occurring on perimeter systems would target the system and not the perimeter.

Other General Comments

One commenter requested clarification why the word "dated" has been added to the measures in these requirements. In response, dated documentation is used to clarify that such evidence is necessary to demonstrate time-based requirements.

There was a comment that suggested the word "annual" should be a defined in the NERC Glossary. In response, the SDT has chosen not to define annual because the periodicity for requirements in CIP may be different than requirements in other standards, and the definition of annual may have many interpretations.

Guidelines

One commenter suggested that references to DHS and NIST should not reside in the standard because NERC does not track those documents to ensure consistency. In response, the external references are dated to a specific version to address the case where future revisions do not remain consistent with the standard.

There was a comment that the definition of Reportable Cyber Security Incident is too vague and could result in the interpretation that activation of redundant systems causes the reporting not to be considered. In response, the SDT has clarified in the guideline that this is not the case. The SDT has added a clarification that the absence of lessons learned must still be documented.

One commenter proposed revisions requirements to "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach and has added to certain requirements "… identify, assess, and correct deficiencies…", which is explained in detail in the global summary portion of this document, above.

Background

One commenter stated that the background section for CIP-008-5 is contradictory in reference to measures by stating a numbered list is all-inclusive but measures serve only as examples. In response, the SDT notes that the background section states "A numbered list in the measure means the evidence example". This means the example evidence must include all of the items, but there may be other examples of evidence to meet the requirement. Both statements are true.

Requirement Part 1.1 and 1.2
Based on a comment, the SDT changed "Processes" to "One or more processes" for clarity.

Several commenters propose including additional specificity in the process for determining if an incident is reportable. The SDT has extensively discussed this issue, and the problem with additional specificity in Cyber Security Incidents is difficulty in exhaustively enumerating situations to report. Also, the reporting of incidents associated with damage alone can result in under-reporting, which does not meet the objective of this Requirement.

Requirement Part 1.4
Several commenters stated that 1.1 (responding) and 1.4 (handling) are essentially the same and proposed to delete 1.4**.** The SDT notes that while 1.1 addresses the initial identification and response to incidents, 1.4 addresses the actions to perform for resolving individual incidents. These are distinct activities.

One commenter suggested the that the applicability include low impact BES Cyber Systems because CIP-003-5 requires implementation of a policy addressing incident response, but CIP-003-5 intentionally centralizes all the requirements for low impact BES Cyber Systems which does not include specific elements of the plan.

There was a comment that suggested removing the parenthetical phrase for incident handling because recovery and post-incident analysis are covered elsewhere. In response, the SDT agrees that post-incident analysis is already handled in Requirement R3 of CIP-008-5 and clarifies the recover activities here pertain only to the incident. Recovery includes the confirmation that the incident has been resolved.

One commenter suggested adding wording to clarify physical security incidents need to be considered. In response, the SDT notes that the definition of Cyber Security Incidents includes physical intrusions.

Requirement Part 1.5

There was a comment that stated it is unclear if the list of internal and external contacts refer to those in EOP-004-2 or if there is a need to have a minimum list of contacts. In response, the internal or external contacts that an entity would need to include to ensure proper reporting for EOP-004-2 should be part of this list. Additional contacts are appropriate as necessary components of an incident response plan, but who resides in this list is left up to the entity.

A commenter suggested that the use of external organizations could result in double jeopardy with EOP-004-2. However, EOP-004-2 requires specific organizations whereas CIP-008-5 leaves the inclusion of additional external organizations up to the entity as a necessary part of the incident response plan. Double jeopardy does not exist here because there is not a requirement in CIP-008-5 to report.

One commenter proposed to replace the phrase "should receive communication" with "must be sent communication". In response, the SDT notes that this part of the incident response plan does not necessarily constitute required communication, but communication must be covered as a component of the plan.

Requirement R2

One commenter proposed adding an exception for the timeframes based on CIP Exceptional Circumstances. In response, the SDT notes that CIP Exceptional Circumstances have not applied to annual periodic performances requirements because of the flexibility in the timeframe of when an entity can perform this requirement.

Requirement Part 2.1

In response to a comment that 2.1 should expand to include all Cyber Security Incidents, the SDT continues to limit these requirements to Reportable Cyber Security Incidents because of the lessons learned and plan updates associated with each Reportable Cyber Security Incident. It is possible for Cyber Security Incidents to occur much more frequently.

In response to a comment, the SDT has removed the word "BES" before "BES Incident Response Plan" for consistency.

One commenter suggested revising the language of "at least once each calendar year, not to exceed 15 calendar months between executions" to "once each calendar year or a period not to exceed 15 calendar months between executions". The SDT notes that the language that exists is sufficient as currently written.

One commenter suggested using the term “exercise” instead of “test” because an actual exercise would suffice. In response, we had several comments to the contrary in the previous posting. The SDT uses test here because the word “exercise” is commonly used in reference to a planned execution.

One commenter suggested removing the lessons learned report from the measure because it is not part of the requirement. In response, we note that the measure only serves as an example, and a lessons-learned report would be an example measure for 2.1.

One commenter suggested that a full operational exercise should be required in the absence of an actual incident. In response, we suggest that the quality of an exercise does not depend on the type. It is possible to have a higher quality tabletop exercise than a full operational exercise.

One commenter suggested placing an “or” between all exercise examples, but this is not necessary because the “or” in the second bullet qualifies the entire list.

One commenter suggested expanding the scope of actual incidents that qualify as an exercise to include any Cyber Security Incident, but this would not exercise a key component of identifying and communicating a Reportable Cyber Security Incident.

One commenter proposed to remove any timeframes associated with the test. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

Two commenters suggested adding a specific reference to R1 to clarify the linkage, but the context of the Requirement in its use of Cyber Security Incident response plan is clear enough to avoid needing a direct linkage.

In response to several commenters, the word “plan(s)” was modified to “each plan” for added clarity.

In response to one commenter, the SDT qualified that the phrase “when responding to” is in regards to the Reportable BES Cyber Security Incident.

Based on comments, the SDT clarified exercises were for Reportable Cyber Security Incidents.

Based on comments, the SDT has removed the word “BES” from this requirement part.

Requirement Part 2.2

One commenter stated that this requirement part should be deleted because the main requirement part already addresses implementation and documented deviations are redundant with lessons learned. In response, the SDT points out that implementation of the plan does not necessarily mean that it be used during an incident or exercise. Some entities may interpret that a plan is implemented regardless of whether or not it is actually used. This additional requirement adds clarity in the expected outcome. The same is also true of lessons learned not having the full meaning of documenting deviations from the plan. However, we agree that the documentation should not necessarily occur concurrent with the incident and have modified this requirement part accordingly.

One commenter suggested requiring documentation for the lack of deviations from the plan. In response, we do not agree this language is necessary. The absence of deviations may be a common occurrence and the requirement to have such documentation is highly administrative. We believe this is different than the case of not having any lessons learned which should be a much less common occurrence.

One commenter suggested requiring plan updates for new vulnerabilities and threats. The SDT agrees this would be appropriate if the plan were not sufficient to address new vulnerabilities and threats, but measurable criteria for what constitutes a new vulnerability or threat does not exist and could likely not be determined by anyone other than the Responsible Entity.

In response to a comment, the SDT replaced the phrase “incident response plan” with “Cyber Security Incident response plan” for consistency.

In response to several commenters, the word “plan” was changed to “plan(s)” for consistency.

Requirement Part 2.3

One commenter proposed that 2.3 should be moved to the compliance evidence section of the standard. In response, the evidence retention section cannot add a new requirement, and without 2.3 there is no requirement to retain evidence of the incident.

Several commenters suggested the language for requirement part 2.3 include a retention period, but this requirement was modified in response to comments that the retention period be covered in the compliance evidence section of the standard. As a result, part 2.3 includes the requirement to retain the records, which may not have been necessary to retain anywhere else in the standard, and the compliance evidence section defines the retention period.

There were several commenters who stated that this requirement part could have double jeopardy with EOP-004-2, but lack of documentation for reporting purposes would not be a violation of CIP-008-5. Also, EOP-004-2 evidence retention does not necessarily cover evidence related to a Cyber Security Incident.

One commenter suggested storing the evidence in encrypted form. In response, CIP-011-1 addresses the storage of BES Cyber System Information. Specific implementation of this requirement is appropriately left to the entity.

The SDT has removed the word "relevant" responding to comments that it adds unneeded subjectivity.

One commenter questioned whether three calendar years is sufficient for retaining incident evidence for law enforcement, state, and federal requirements, but the evidence retention is a minimum for the purpose of the Standard. If additional requirements outside of the NERC Reliability Standards indicate a longer retention period for a particular entity, then the entity would choose the longer period. There is no conflict.

Requirement R3

One commenter proposed that the main requirement should more closely align with CIP-009-5 R3 and focus on maintaining, and not implementing, the plan. The SDT agrees.

One commenter suggested the word "full" be deleted from "full operational exercise" because it is unclear what it implies. The SDT agrees.

Requirement Part 3.1

Several entities have commented this requirement part is duplicative with testing in R2 and monitoring for plan changes in R3. The SDT agrees and has deleted this requirement part.

In response to a comment that proposed to consider additional changes that trigger a review of the incident response plan, the lessons learned requirements suffice for updating the plan in response to incidents. Changes to the security

configuration already trigger updates in requirement part 3.4. In many cases the incident response plan is written at a high enough level to preclude necessitating changes in response to new threats and vulnerabilities.

Requirement Part 3.2

There were several comments that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.2, 3.3 and 3.5 into a single requirement part 3.1. The additional requirement part 3.4 for monitoring plan changes and 3.5 has collapsed into a single requirement part 3.2. Some commenters suggested that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

One commenter suggested tying this requirement explicitly with both 2.1 and 2.2. In response, the cross-referencing of requirements could cause more confusion than clarity. The SDT feels this explicit tie is best accomplished in the guidance.

One comment proposed to remove any timeframes associated with plan updates. The SDT disagrees because absence of time requirements makes the expected performance of the standard less clear and does not respond to directives from the FERC Order 706.

There was a comment that suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

One commenter suggested changing this requirement part to include language for consistency with the ERO Event Analysis Process. The ERO Events Analysis Process is not a NERC Reliability Standard, and the SDT is not mandating referenced actions that are not developed through the NERC process or an equivalent ANSI Certified process. The SDT also notes that the proposed requirement language leaves flexible “how” to perform the requirement. Entities may choose to follow the procedures outlined in the ERO Events Analysis Process to comply with the requirement, but are not required to. The SDT also understands that the NERC CIPC is planning to form a working group to develop guidelines for analyzing cybersecurity events using a parallel process to the recently approved ERO Events Analysis Process. Specifying

that the ERO Events Analysis Process be used in response to CIP-008 Reportable Cybersecurity Incidents is premature and will remove any perceived or required flexibility in developing cybersecurity-specific procedures under that group.

Several commenters suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

In response to one comment, the SDT has added examples of evidence for lessons learned.

In responses to multiple comments, the SDT changed the phrase “within 90 days” to “not to exceed 90 calendar days” for clarity.

Requirement Part 3.3
In response to a comment, it is not necessary to modify this requirement to state “update as needed” because the requirement part ties to “any lessons learned” which carries the same effect.

Requirement Part 3.4
One commenter suggested reverting to previously approved language for updates and notes that evidence to meet this requirement would include lists of technology changes. In response, the SDT notes that such evidence would be required in the previously approved version if specific technology was referenced in the plan. The changes identified here are to provide additional clarity in the types of changes that should trigger an update.

Several commenters proposed that the term “technology changes” needs to be defined. The SDT notes this only includes technology changes that would impact the ability to execute the plan. Because this term is so contextual to the plan, it would cause more problems to define it. Entities should review their plans to see whether or not they have technology as a key element of the plan. The guidance specifies that “technology changes affecting the plan may include referenced information sources, communication systems or ticketing systems.”

Requirement Part 3.5
Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the evidence examples of distributing the plan could result in a violation of confidentiality, but, while each example can specify additional mechanisms to preserve confidentiality, this was not the intention of the measure. In some cases, incident response plans may not contain confidential information.

VSLs

One commenter recommended that the documentation of the absence of any lessons learned should be included in the VSLs. In response, the absence of lessons learned has been included in the VSL.

One commenter recommended that the VSL should not include failure to follow the plan during an incident and the VSL associated with lack of documentation of deviations suffices. The SDT agrees and does not need to modify the VSLs.

QUESTION C8 – CIP-009-5:

If you disagree with the changes made in CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-009-5 expressed in comments were (1) backup media verification procedures in requirement parts 1.4 and 2.2, (2) data preservation procedures in 1.5 and (3) timeframe requirements in Requirement R3 on the lessons learned and plan update activities. The consideration of comments according to major issues and standard sections follows.

Applicability

One commenter suggested that the applicability for all requirements in this standard should limit to Medium Impact BES Cyber Systems at Control Centers to appropriately focus on the higher risk cyber systems and avoid conflict with PRC Standards. In response, the loss of Medium Impact BES Cyber Systems has impact to the BES and the recovery operation for these cyber systems should be addressed in this standard.

The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs, which means testing for substations and generating plants that are not high impact is not included. A commenter asked for confirmation on whether this was the SDT's intent. Yes, it was.

One comment suggested that applicability to associated Cyber Assets should be removed because the FERC has not directed to do so. In response, these continue to apply from all prior versions to the associated Cyber Assets.

Other General Comments

One commenter proposed modifying the main requirement part and corresponding VSLs for R2 and R3 to allow for a flaw remediation process. In response, we have modified the main requirement part for R2 to eliminate the zero tolerance obligations because of the possible magnitude of plans and backup media which require testing. However, we do not incorporate the same changes for R3 because the requirements here do not have the same zero-tolerance concerns and they specify the procedures that must be in place to ensure better response plan flaw remediation.

Guidelines

Several commented that application guidelines should be included for CIP-009-5, and we have added these.

Background
One commenter suggested that the background section is contradictory by saying that measures are not all-inclusive but numbered list provide an all-inclusive example. In response, the background section states, "A numbered list in the measure means the evidence example includes all of the items in the list." This refers to the single example and is different than an all-inclusive list of evidence examples. Accordingly, if an entity did not provide all parts of the numbered list of evidence, then they would not fully meet the requirement. However, they could still provide alternate forms of evidence outside of the example.

Measures
There was a comment that the measures should be clarified with the following language: "Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." The SDT notes that the language in the requirement is clear and that the measures provide adequate examples of evidence. Each requirement part addresses different levels of that may be expected.

Requirement R1
One comment proposed to add a requirement for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. They also commented that the requirement should state the level of granularity required for a plan. In response, it would be problematic to standardize and audit a normal operating role. The SDT is uncertain as to the meaning of this term. The purpose of this standard is "to recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES." It is inappropriate to specify the level of detail required for a recovery plan.

Several commenters suggested that the standard is not clear whether the recovery plans are for recovery of the asset, system, or function. In response, the stated purpose for the standard is "to recover reliability functions performed by

BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES."

One commenter asked the following: "is a Business Continuity Plan, where operations are transferred from the main control center and continued at a back-up control centre, considered a recovery plan?" In response, this could constitute a recovery plan according to Requirement R1 with the additional components listed in the requirement parts. However, restoration of the reliability function meets the purpose of this standard.

Requirement Part 1.1
One commenter suggested removing "specific" activations from the measure, and we have done so.

One commenter suggested the minimum conditions for activating a response should be specified. Otherwise entities can choose an inappropriately high bar. In response, any minimum enumeration of recovery conditions would equate to defining system failure and doing so for a highly variant population of systems across the BES is not feasible.

Requirement Part 1.3
Several commenters suggested changing the phrase "BES Cyber System" to "applicable Cyber Assets". However, "restoring BES Cyber System" functionality describes the objective of the requirement part and not the applicability.

One commenter suggested addressing FERC Order 706 paragraph 748 by appending the suggested text from the Order to this Requirement Part addressing backup media. We agree this is clearer and have incorporated their suggestion in requirement part 1.4 because of the difference in applicability from 1.3.

One commenter suggested modifying this requirement part measure to provide alternate forms of evidence and avoid the interpretation that evidence must be shown for each occurrence in a high-frequency operational requirement. In response, the SDT has modified the measure according to these suggestions.

Several commenters suggested removing the qualifier word "successfully" from the measure and the SDT has done so.

One commenter suggested including documented configuration settings, documented build/restoration procedures, and retention of installation media for example evidence. The SDT has added these to the technical guidelines section of the standard.

Several commenters suggested replacing the word “recover” with “restore” to describe the purpose of the backup media. In response, we retain the use of “recover” to avoid confusion. Both words mean to return something to a normal or former condition, and the SDT finds these words can be used interchangeably while still communicating the same concept.

One commenter noted the measure is missing an “and”, and the SDT has corrected this oversight.

Requirement Part 1.4

Several commenters expressed confusion around the term “initially” in the requirement, and the SDT has removed this term by tying the verification processes to the backup and storage processes in 1.3. The resulting language should provide more clarity and eliminates the term “initially”.

One commenter suggested addressing FERC Order 706 paragraphs 732-734 in this requirement section or moving this to guidance. In response, the resulting directive in paragraph 739 is addressed by the proposed text to address 748. Another commenter also supported the proposed language in the FERC Order. In response, verifying the operability of backup media is addressed by verifying successful completion and addressing failures of the backup process. Short of performing a full restoration, monitoring the backup process provides the appropriate assurance in the integrity of the backup for constantly changing systems. We have also added further guidance for this requirement part.

One commenter stated that FERC did not express concern over Physical Access Control Systems and Electronic Access Control and Monitoring Systems and applicability for these should be removed. In response, we retain the applicability from previous versions of the standard to which the FERC Order was addressed.

Several commenters requested further clarification about the meaning of verification of backup media. In response, the verification of backup media is dependent upon the tool performing the backup. This could include checking for read/write errors or performing a checksum during the backup operation. The SDT has clarified this requirement to read verification of successful completion.

One commenter suggested this requirement part be modified to address 3rd parties performing the backup or providing a backup, and the requirement has been modified to address these concerns.

Several commented on the 90 day retention period for the logs specified in this requirement part measure. In response, the reason for having 90 day retention for BES Cyber System logs is the potentially large volume, but there is no such concern for the evidence example for this requirement part.

One commenter does not believe this requirement part belongs as written here, and we note the overall modifications to this requirement part better fits the overall objective of Requirement R1.

One commenter stated that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to regularly verify the redundancy and address failures.

One commenter asked the following questions: If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? In response to these questions, the currently proposed requirement does not specify a timing that is sufficient for verification due to the widely varying backup methodologies that exist for the applicable systems. A printed log or periodic automated sampling of the backup process would be considered sufficient evidence for this requirement.

One commenter stated that the only way to verify backup completion is to restore from backup. In response, completion of the backup process or routine is different than successful restoration, and we contend the former can be verified outside of a full restoration.

Requirement Part 1.5

Several commenters suggested replacing the word "event" with the phrase "Cyber Security Incident" to better scope when it is necessary to preserve data. In response, we have made this change and modified the requirement to better qualify the purpose of preservation. The requirement should read clearly that data must be retained until a Cyber Security Incident may be ruled out as the cause of the recovery operation.

One commenter suggested removing this requirement part because it addresses forensics and not recovery. In response, this requirement part ensures data collection procedures are included in the recovery plan to allow the performance of after-the-fact analysis. This is appropriate to require as part of the recovery operation.

One commenter suggested that with changes to the definition of CIP Exceptional Circumstances to include "an imminent or existing hardware, software, or equipment failure", this requirement would never invoke. Their proposed language incorporates the concept of CIP Exceptional Circumstances, and we have included much of the proposed wording in the revised requirement part. The commenter also proposed to limit this requirement part to Medium Impact BES Cyber Systems at Control Centers, but neither the threat nor the operational circumstances for field assets preclude applicability for this requirement part. This requirement allows sufficient flexibility to apply in widely varying environments. The modifications here also address other comments about clarifying the procedures should not impact reliability.

One comment suggested that the PRC Standards already cover this for relay misoperation, but these standards do not address specifically the failure of a Cyber Asset nor do they address the preservation of data from Cyber Assets.

One commenter stated that this requirement implies an obligation to mirror data in the measure, should be left up to the entity to determine whether or not to delay recover for the purpose of preserving data, and an entity cannot determine the preservation of data given the many ways in which a system can fail. In response, we first note that a measure is only an example and does not imply an obligation to mirror data. Second, the SDT has taken an exception to add an explanatory note in the requirement cautioning against impeding recovery for data preservation. Finally, this requirement part does not envision an entity determining every way in which a Cyber System can fail. This only obligates the entity to include data preservation procedures in the recovery plan. There was a second comment on the guidance language in the measure, and the SDT agrees the language does not readily associate itself to the requirement and has been removed.

One comment suggested that this requirement part should be part of root-cause analysis and not impede system restoration. The SDT agrees and notes the requirement part does not address forensics but only the preservation of data to support root-cause analysis and forensics after-the-fact.

Requirement Part 2.1

One commenter suggested for this requirement part and requirement part 2.3 that the word “exercise” should be used in place of “test” since an actual recovery operation can be used for compliance. However, several commenters suggested the converse in the last posting, and we are not compelled the difference in terminology changes the meaning of the requirement.

One commenter suggested revising the language of “at least once each calendar year, not to exceed 15 calendar months between executions” to “once each calendar year or a period not to exceed 15 calendar months between executions”. The SDT notes that the language that exists is sufficient as currently written.

Several commenters requested clarity about whether or not each recovery plan must be tested annually. In response, we have modified this requirement to explicitly state that each recovery plan must be tested as was the intent. We do not specify a representative sampling of plans be tested as some suggest because the proposals do not include enough information to objectively determine what constitutes a representative sample. However, we do note that it is possible to singularly test multiple cyber systems if they are similar in nature.

One commenter suggested that all backup media should not be required for testing but only the one needed for recovery, and we have modified the requirement to include this condition.

One commenter suggested that “or” should be added to the first bullet point or it is otherwise required. In response, the or in the second bullet point modifies the entire list.

Requirement Part 2.2

One commenter asked if this requirement part includes a media test and whether this can be performed on a sample system. In response, this can include a media test on a sample system provided some verification to ensure the information is current and useable occurs. We have modified the measure for this requirement part to make this clearer.

One commenter suggested allowing an actual recovery operation to substitute for the testing of backup media, and we have made this change.

One commenter proposed to replace the requirement with “Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar

year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable." The concern surrounds possible double jeopardy with EOP-008 and clarity around "compatibility with current system configurations." In response for EOP-008-1 R7, failure to meet this requirement does not indicate a failure for EOP-008-1 and vise-versa. This requirement concerns the testing of backup media, which may not be used for recovery with EOP-008-1. For the proposed language, we have incorporated the "representative sample of information" in testing to clarify the obligation, but we retain the purpose of verifying compatibility with current system configurations. Only ensuring the usability of backup media does not capture the intent that the backup media is currently usable for performing the BES Cyber System function.

One commenter suggested striking the phrase "to ensure that the information is useable and is compatible with current system configurations" and believes it should be left up to the Responsible Entity to determine, whether another commenter requested further clarification about this phrase. In response, the testing of backup media alone is not specific enough to ensure clarity of the requirement. The phrase in question is necessary for entities to know what they should be testing. We have added additional technical guidelines for this requirement.

One commenter suggested that this requirement should state that a tabletop exercise should not be permitted. In response, the testing of backup media may be performed as a separate process or as a part of the recovery plan exercise. There is not a need to specify which type of exercises aligns with this process.

One commenter suggested that the term "backup media" is antiquated and should be replaced with redundancy terminology. In response, we disagree the term is antiquated, but if redundancy is being used for recovery, then processes should exist to test the redundant systems in accordance with this requirement part.

Several commenters proposed the phrase "validate the integrity of the stored information" as a substitute for current language regarding the testing of backup media. In response, validating the integrity of the information can be interpreted widely from a bit comparison to a sampling. We believe our proposed revisions provide enough specificity and flexibility to be widely applied.

One comment proposed to focus the requirement on backup media rather than information used for recovery. In response, we use the term information here because of the various ways entities implement backup policies, which may include replication technologies. Backup media was not well understood by the team and many participants to include replication.

Requirement Part 2.3

Several comment that the measure references performance of this requirement prior to the Effective Date, and that this requirement part should be included in the Implementation Plan. In response, we have removed this language from the measure and added this requirement part to the Implementation Plan.

One commenter suggested testing a representative of a plan with a rationale that High Impact BES Cyber Systems already have a requirement to test backup media annually. In response, we do not see a significant change in the proposed wording. The requirement to test backup media does not require a full operational restoration.

One commenter requested clarity that all recovery plans do not have to be tested at the same time. In response, the requirement only specifies the obligation to test recovery plans at a periodicity. It would not violate the requirement to test individual plans at different periods while still meeting the periodicity obligation.

One commenter requested a basis for the 36 months period. In response, we incorporated this timeframe from the FERC Order 706 directive.

One commenter suggested testing a “representative” rather than “each” BES Cyber System. In response, if an entity can test a representative BES Cyber System for multiple systems, then they have complied with the requirement to test “each” BES Cyber System.

One commenter noted that an entity may have several failure scenarios and it is unclear if all of these must be tested. In response, we have added guidance in the technical guidelines section of the Standard to clarify that not all failures scenarios must be tested, but that the test should ensure the plan is up to date and test at least one process to restore the applicable cyber systems.

One commenter suggested that EOP-008 R6 should suffice for this requirement part. In response, EOP-008-1 R6 requires independent backup functionality, but this does not imply an obligation to perform a functional test. The compliance processes to comply with EOP-008-1 should certainly ease compliance with this requirement part.

Several respondents asked whether a full operational exercise means a bare-metal recovery and comments that doing so would be cost prohibitive, while another commenter suggested also requested further clarification around

the term “operational exercise”. In response, the SDT has provided well established definitions of operational exercises that would comply with the requirement, which do not imply a full recovery demonstration.

Requirement R3

Requirement R3 has been modified to correspond with similar commenter suggestions in CIP-008-5 R3.

One commenter suggested that Requirement R3 does not include defined roles and responsibilities. As we understand the comment, the roles and responsibilities refer to those required parts of the response plan specified in Requirement R1.

Requirement Part 3.1

Several commenters noted that the various dates for updating the plan significantly increase the compliance tracking burden and that a plan has not truly updated until the entity distributes those updates to the required individuals. The SDT agrees and has collapsed previously posted requirement parts 3.1, 3.2 and 3.4 into a single requirement part 3.1. The additional requirement part 3.3 for monitoring plan changes and 3.4 has collapsed into a single requirement part 3.2. Some comment that both requirements should allow a consistent 90 days, but the updating of the plan in response to changes does not require the same level of updates as those required from lessons learned. Therefore the different timeframes in these requirement parts are appropriate.

A few commenters suggested updating plans based on lessons learned is not necessary because these changes would be captured in technology and personnel changes. In response, the updates here capture improvements to the plan as determined through a lessons learned exercise.

One commenter suggested that the evidence collected in requirement part 1.5 should be part of the review process. They also commented that other related plans (i.e. configuration management plans) be updated as necessary as part of the review process. In response, the evidence collected in requirement part 1.5 may not be reviewed by a third party and we do not feel it is necessary to specifically call out this activity in the requirement part. Also, we cannot add an obligation to update other plans as necessary in a way that would be objectively measurable.

One commenter suggested that 30 days may not be sufficient time to make complex changes from lessons learned. In response, the SDT believes the updated requirement allowing 90 days for the complete time is sufficient for even complex changes.

Several commenters have suggested clarifying the expectation when there are no lessons learned. In response, we have made this explicit in both the requirement and measure.

Several commenters stated that requiring entities to perform lessons learned is counterproductive because it encourages entities not to admit there is a deficiency in the first place. In response, the inclusion of a lessons learned process provides a standard practice across the industry, which would otherwise be inconsistency applied at best. Furthermore, it addresses a FERC Order 706 directive to include lessons learned processes as part of a recovery plan test.

Requirement Part 3.3

One commenter suggested modifying the references to other standard requirement parts, removing references to individuals and modifying the communication of plan updates to be more specific. In response, the SDT has made several modifications to Requirement R3 to align with modifications to CIP-008-5 that address these concerns.

Several commenters proposed removing this requirement and addressing plan updates in guidance, but placing the plan items that would trigger a change in guidance would add a high degree of subjectivity to the requirement. Specifying what changes should constitute an update ensures objectivity in demonstrating compliance with this requirement.

One commenter proposed removing this requirement or clarifying the tie back to Requirement R1.2. In response, this requirement is necessary to ensure the recovery plan remains current and carries forward from the requirement to update on any changes. They also expressed concern that this requirement part could be interpreted that a change to any plan must be communicated to all individuals specified in requirement part 1.2. In response, we have removed the explicit tie to requirement part 1.2 to avoid such an interpretation.

One commenter suggested that the plan maintenance would create an undue compliance burden. In response, the SDT notes this requirement carries forward from previous versions and ensures the recovery plans remain up to date through organizational changes.

Requirement Part 3.4

Several commenters suggested changing the word “distribute” to “notify” for announcing changes to the incident response plan due to the uncertainty of what constitutes distribution and the possible issues with information sensitivity. The SDT agrees.

One commenter suggested the distribution of plan updates should include some irrefutable evidence on the part of the receiver. In response, we do not believe the added qualification would have the desired benefit. Individuals can choose to ignore the content regardless of the evidence of receipt.

One commenter stated that the example evidence for communicating plan updates is a poor choice because of the confidentiality of such information. In response, the examples do not necessitate the sharing of sensitive information but only that the individuals be notified. We have included additional guidelines to consider the sensitivity of the information when sending the required notifications.

VRF

One commenter proposed that the VRF should be Lower for consistency with other requirements. In response, we retain the previously FERC approved VRF of Medium for this requirement because failure to have restoration procedures directly affects the BES reliability function of High and Medium impact BES Cyber Systems.

VSLs

The VSLs have been updated corresponding to changes made to requirements in CIP-009-5.

One commenter suggested that “within 30 days” should be changed to “greater than 30 days”. The SDT agrees and has made this change.

Several commenters suggested that the moderate VSL for Requirement R1 should address “one” and not “all” missing elements of the plan. The SDT agrees and has made this change.

One commenter suggested that the VSL for Requirement R3 should capture not documenting the absence of lessons learned. The SDT agrees and has made this change.

One commenter proposed to replace the Requirement R3 VSLs with graduation from 90-210 days beyond the required obligation. The SDT agrees and has made this change.

One commenter noted the graduation of VSLs for requirement part 2.2 incorrectly lists a period of within 19 calendar months for the Severe category, and the SDT has modified this to be 18 calendar months.

QUESTION C12 – CIP-010-1:

If you disagree with the changes made in CIP-010-1 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the primary concerns regarding CIP-010-1 expressed in comments were (1) references to CIP-005, CIP-006, and CIP-007 within CIP-010, (2) scope of baseline configuration items in R1.1, (3) applicability including associated assets/systems and also including "external routable connectivity" language, (4) requirement language above and beyond FERC Order 706, and (5) other requirement and measure language modifications. The sections below are a summary of the comments received and include SDT responses for CIP-010-1.

CIP-010-1 General Comments

Many commenters requested an explanation for why CIP-010 depends on CIP-005, CIP-006, and CIP-007. Based on previous requirements in older versions of CIP-003, CIP-005, and CIP-007 (CIP-006 has since been removed from requirement language), the SDT combined the various requirements related to configuration change management and vulnerability assessments to create CIP-010. Both configuration change management and vulnerability assessment require validation that controls from CIP-005 and CIP-007 are not affected. Therefore, CIP-010 references CIP-005 and CIP-007. The SDT does not believe this cross-referencing creates a "double jeopardy" situation. Whether the requirement existed in CIP-005 or CIP-007, if an issue is discovered, then the issue would be a violation of where the requirement was enforced (CIP-005 or CIP-007) rather than in the requirement which enforced the search for issues (CIP-010). New "identify, assess, and correct deficiencies" requirement language will also aid in compliance concerns.

Several commenters mentioned that they desired a return to the approved language in CIP-003-4 Requirement R6 and CIP-007-1 Requirement R1 with targeted and efficient changes to address the FERC order. Another commenter further recommended a return to the draft 1 language. The SDT disagrees with their determination and believes that the current CIP-010-1 language is proper and in order. Based on this commenting period, the SDT has revised language for clarity and consistency. Language was also modified in an effort to address industry comments.

Numerous commenters recommended that all references to Medium Impact BES Cyber Systems in CIP-010 applicability include: "with External Routable Connectivity." The SDT does not agree with the addition of External Routable Connectivity to CIP-010 applicability. Whether a cyber asset has some type of connectivity or not, it can still be pervious

to vulnerabilities (i.e., Stutnex). The SDT's determination is in accordance with FERC Order 761, Paragraph 86. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010.

One commenter proposed removing from the measures: "… and the output of the tools used to perform the assessment," since this is thought to be a part of CIP-010-1 Requirement R3.4. The SDT does not agree with this modification since CIP-010-1 Requirement R3.4 asks for the results of the assessments, while CIP-010-1 Requirements R3.1 through R3.3 are referring to the output of any tools used to perform the assessment. In consideration of this comment and other industry comments, the SDT included "any" to the requirement in the case that no tools were used to perform the assessment.

Several commenters suggested the removal of: "… but not limited to …" in CIP-010 measures. The SDT has modified measure language in consideration of their comment. The SDT also emphasizes that the: "… but not limited to …" is supposed to benefit the responsible entity and not create an item for auditors to use against them.

Multiple commenters suggested that specific controls from CIP-005 and CIP-007 be identified in CIP-010-1 Requirements R1.3, R1.4.1, and R3.1 so there would be no need for interpretations. These comments were taken into consideration, and the related requirement sub-parts were modified accordingly. The references to CIP-005 and CIP-007 were removed from some requirement sub-parts. Also, per consideration of these comments, CIP-006 was removed from requirement language where the language was present.

One commenter believed that some requirements in CIP-010 expand the scope and documentation burden beyond earlier CIP standards versions due to CIP-005 and CIP-007 references. In consideration of these comments, the SDT has modified CIP-010-1 Requirements R1.3 and R3.1 accordingly. References to CIP-005 and CIP-007 have been removed from the sub-part requirement language. It should be noted that the SDT disagreed to removing these references in Requirement R1.4.1. The SDT also added the reference to Requirement R1.5.1 for consistency across Requirement R1.

One commenter recommended adding a reference to the associated requirement part in which each CIP-010-1 VSL is related. The VSLs are written at the higher-level requirement, but do include elements that refer to the various requirement parts. Therefore, the SDT does not believe that the associated requirement part needs to be included in the VSL. One commenter continued to suggest that the VSL language should more closely mirror the requirement language. The SDT has taken into consideration this comment and modified the VSL language accordingly.

One commenter mentioned that having a documented baseline and monitoring it closely makes the vulnerability assessment prior to deployment have no benefit. The SDT does not agree with this assessment, as a vulnerability assessment is more than just monitoring for changes to the baseline. Please see the guidelines section of the standard for CIP-010-1 Requirement R3. Also, other commenters mentioned that establishing a production-like environment that could produce an active vulnerability assessment would be difficult and expensive. The SDT added the language: "… production environment where the test is performed in a manner that minimizes adverse effects …" for instances when a test environment is not available.

One commenter recommended an expanded glossary of the many terms used in CIP-010. The SDT has taken this comment into consideration and has expanded upon the guidelines to include more guidance around terms related to the baseline configuration and cyber security controls.

One commenter recommended further items to be incorporated into the baseline configuration; including communication protocols, non-standard BIOS configurations, and other items. The SDT believes that the requirement language is sufficient as written, as adding additional items into the baseline configuration at this time period would be difficult to support consensus.

One commenter recommended that CIP-010-1 have an effective date that is 12 months after the effective date of the CIP V5 standards. The SDT will take this comment into consideration, as this comment references the Implementation Plan and not necessarily language within the CIP-010-1 standard.

One commenter commented on the use of the term "Configuration" versus "configuration." The SDT has revised CIP-010-1 to only use "configuration," since it was not the SDT's intent to include "Configuration," as this is not a NERC defined glossary term. Furthermore, another commenter questioned if the terms: "configuration management," "configuration change management," and "asset management" were synonymous terms. The SDT has revised CIP-010-1 to only use "configuration change management" for less confusion. "Asset management" is not synonymous with the other words in the previously mentioned sentence. "Asset management" where it is used (R1.1 measures) refers to SAP, Maximo, Cascade, Passport, or other asset management software. Also, due to other questions around the baseline configuration, the SDT has added further guidance to aid in entities' development of their baselines.

Applicability Section

A couple comments mentioned that the exemption language in Section 4.2.4 should be changed back to the previous ballot's CIP-010-1 language or this section should be struck if it truly only applies to CIP-002-5. The difference between the initial ballot posting and successive ballot posting is 4.2.3.5, which states that: "Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes."

One commenter recommended the striking of the applicability component of the main requirement. If the commenter is referring to Section 4 of CIP-010, then this section is required for NERC standards to identify the standard's applicability to Responsible Entities, while the (newly termed) "applicable systems" columns in the tables refers to the scope of systems to which a specific requirement row applies.

Many commenters recommended removing some or all associated assets/systems from various applicability sections in the CIP-010 requirements because they represent an increase in scope from CIP V3/V4. The SDT disagrees with this assessment, as CIP Version 3 and Version 4 standards mention applicability to cyber assets within the ESP. The cyber assets that could exist within an ESP would include Associated Protected Cyber Assets, Associated Electronic Access Control or Monitoring Systems, and Associated Physical Access Control Systems. Therefore, the SDT does not believe that the assets/systems from CIP-010's applicability represent an increase in scope from CIP Version 3 and Version 4 standards.

One commenter expressed concern over 4.2.2, bullet 3, which references: "… Transmission where the Protection System is required by a NERC or Regional Reliability Standard." The concern was that CIP-010-1 was requiring the installation of a Transmission Protection System. This assessment is incorrect. CIP-010-1 does not require the installation of a Transmission Protection System, but other NERC or Regional Reliability Standards may require the installation of a Transmission Protection System.

Guidelines Section

Several commenters suggested adding the phrase: "network connectivity to identify" to the Requirement R3 guidance with regard to passive network discovery. The standard has been modified in consideration of these comments to include the phrase. One commenter made several other suggestions (such as the addition of details on baseline configurations and cyber security controls) in regards to guidance that informed the SDT's modification of that section.

Background Section

Several commenters mentioned that the third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. The SDT believes that this third paragraph is clear in stating:

- A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence.
- The word "required" is not used to describe numbered or bulleted lists. The SDT wishes to emphasize that measures are only examples of evidence.

Requirement R1

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has added the "in a manner that identifies, assesses, and corrects deficiencies" language to the requirement, which is described above.

One commenter proposed that the requirement be changed to a program- or performance-based level to allow more flexibility (citing FERC FFT Order, Paragraph 81). The comment furthermore mentions that programs such as Tripwire would not be able to be used. Other commenters had similar comments in regards to the prescriptive language of CIP-010-1 Requirement R1.1. Based on the revised "identify, assess, and correct deficiencies" language, the SDT believes that more flexibility is achieved through an entity's internal controls process. Furthermore, the SDT believes that programs such as Tripwire could be used to aid in compliance with CIP-010-1 Requirement R2.

One commenter believed that information in Requirement R1 should only be collected for personal computers and protective relays. The SDT disagrees with this comment, as the applicability should involve all BES Cyber Assets, BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems since these assets can be found within the same Electronic Security Perimeter.

One commenter asked if recording software "hashes" can be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset. The SDT attempted to provide flexibility to allow the entity to determine how to track changes. However, in regards to CIP-010-1 Requirement R1, the baseline configuration still must be documented. If an entity is able to use software "hashes" to monitor for changes to the baseline configuration of a BES Cyber System, then this solution could be used for CIP-010-1 Requirement R2.1.

One commenter proposed a modification to language in CIP-010-1 Requirement R1 to eliminate the term "baseline" so that it is not confused with the security baselines that they create today for devices. Two other commenters also wanted to remove the "baseline" from CIP-010-1 requirement language. The SDT disagrees with the proposed change and believes that the language, as is with the term "baseline," is sufficient.

Requirement Part 1.1

A few commenters emphasized that Version 4 did not apply to noncritical; but in accordance with FERC Order 761, Paragraph 86, these assets/systems should be included in CIP-010-1 Requirement R1.1. Therefore, external routable connectivity exclusion language was not included in the applicability for CIP-010-1 Requirement R1.1. Numerous commenters also alternatively recommended that CIP-010-1 Requirement R1.1 applicability only include High Impact BES Cyber Systems. The SDT disagrees and continues to cite FERC Order 761, Paragraph 86.

Several commenters disagreed with the use of the phrase: "… each Cyber Asset identified, individually or by group." The SDT has revised the requirement language in regards to their comment so as to ensure baselines can be defined at the individual or group level.

One commenter also desired a clarification of what may be grouped under CIP-010-1 Requirement R1.1. The SDT hopes that the revised requirement language provides additional clarity.

Requirement Part 1.1, Sub-Part 1.1.1

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Several commenters recommended replacing "exists" with "is either operating or running." Another commenter believed the wording of "is installed" is also sufficient. The SDT wants to underscore that "exists" refers to the case when an asset has firmware instead of an Operating System.

Requirement Part 1.1, Sub-Part 1.1.2

One commenter mentioned that "BES Cyber Asset" should be replaced with "applicable Cyber Asset." Other commenters had a similar position with regards to the use of "BES Cyber Asset." These comments were taken into consideration and

the related requirement sub-part was modified. The phrase “on the BES Cyber Asset” was removed from the requirement sub-part for consistency.

Multiple commenters requested clarification on the “applications.” Does “applications” mean “SCADA, EMS, State Estimator, etc.” instead of “device drivers and DLL applications” included in an operating system or package?” In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

A couple commenters suggested the removal of the word “intentionally” from the requirement language. The SDT believes that the use of the term “intentional” was meant to ensure that only software applications that were determined to be necessary for cyber asset use should be included. It is not the SDT’s intent for notepad, calculator, DLL, device drivers, or other applications included in an operating system package to be considered as commercially available or open-source application software. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities requested clarity on how granular the version identifier should be. The SDT provides flexibility for entities to determine what version levels should be tracked. The purpose of tracking the version allows entities to keep abreast of the version levels in their inventory. If software manufacturers alert entities to vulnerabilities in their software, the affected population could be identified through software version. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Several entities suggested that sub-part 1.1.2 should exclude anti-malware signature file version identifiers due to the volatility of frequency updates. The SDT believes that only version levels that can aid in recognizing affected software should be tracked. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

Requirement Part 1.1, Sub-Part 1.1.3

Multiple entities asked if a version control tool/system (like Concurrent Versions Systems) could demonstrate the custom software's version. In consideration of these comments, this requirement sub-part has been reworded to be "custom software installed." However, even in its successive ballot form, the requirement sub-part did not require the custom software version. Instead, the requirement sub-part requires the identification of the custom software.

One commenter believed that this requirement is covered in CIP-009 Requirement R.1.3. The SDT disagrees with this comment, as the process for the backup and storage of information required to recover BES Cyber System functionality is not required to include baseline configuration items.

Multiple commenters suggested removing "developed for the entity." The SDT has taken this comment into consideration and modified the requirement language accordingly.

There were several commenters who proposed modified language to clarify the term "custom software." The SDT disagrees with these proposed changes, but has reworded the requirement language in an attempt to provide additional clarity.

Requirement Part 1.1, Sub-Part 1.1.4

There were many commenters who believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what patches should be installed, while CIP-010 handles the patch being implemented (i.e., going through the configuration change management process).

One commenter believed that CIP-010-1 Requirement R1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Only ports which are accessible need to be included in the baseline. In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter asked for clarity around "logical network accessible ports." In consideration of these comments, the SDT has added additional detail to guidance in regards to baseline configuration items.

One commenter mentioned that the applicability columns from CIP-007 should match the applicability column in CIP-010-1 Requirement R1. The SDT does not agree with this comment, as the concept in CIP-010 is to identify logical network accessible ports, while CIP-007 requests entities to enable logical network accessible ports.

Requirement Part 1.1, Sub-Part 1.1.5
One commenter mentioned that CIP-010-1 Requirement R1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. This comment was taken into consideration and the related requirement sub-part was modified.

Many commenters believed that this requirement is covered in CIP-007. The SDT remarks that CIP-007 is evaluating what should be used, while CIP-010 is the implementation.

One commenter believed that CIP-010-1 Requirement R1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. Only historic or current patches that have been applied would be included in the baseline.

Several comments raised the concern Requirment R1.1.5 changes too frequently to be in the baseline and should be removed; that the evaluation of each patch is already included in CIP-007-5. The SDT believes that CIP-010-1 Requirment R1.1.5 is supposed to be a comprehensive listing of the patches that have been installed on the device. Patches are not required to be evaluated with this requirement. Instead, if a patch has been added to the device, then an update of the baseline is required.

Measures for Requirement Part 1.1
Per a comment, “or group” was added to CIP-0101 Requirement R1.1 measures to make consistent the requirement language and measures.

Requirement Part 1.2
One commenter proposed a rewording of CIP-010-1 Requirement R1.2 to: “Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware.” The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP Version 5 requirement language.

One commenter proposed indicating the appropriate authorizing individual or delegate in the requirement. The SDT believes that the requirement is sufficient, as is since it provides flexibility so that the entity can select the appropriate authorizing individual.

Measures for Requirement Part 1.2

One commenter recommended the removal of language in measures around individuals or groups with the authority to authorize the change. The SDT believes that measures are only examples of evidence. To be in compliance with the requirement language, an entity could authorize change by an individual, a group, or other entity-determined method.

There were two comments that recognized a concern with the language: "Documentation that the change was performed in accordance with the requirement." There was another suggestion to remove this language since it is not clear to what term the requirement is referring. The SDT believes that since the measure is for CIP-010-1 Requirement R1.2, that the language in the measure directly refers to CIP-010-1 Requirement R1.2 language only. While the SDT considered adding a reference to CIP-010-1 Requirement R1.2 in the measure to make explicit the requirement to which the measure language was referring, for consistency across CIP-010, this change was not made.

Requirement Part 1.3

One commenter mentioned that the applicability columns from CIP-005 and CIP-007 should match the applicability column of CIP-010-1 Requirement R1.3. This comment was taken into consideration and the related requirement sub-part was modified accordingly. The reference to CIP-005 and CIP-007 was removed from the requirement sub-part; and, therefore, the applicability columns between the standards do not need to be consistent.

There were many commenters that expressed concern with the 30-day time frame. Other commenters recommended the removal of the 30-day time frame for updating the baseline configuration. The SDT disagrees with the commenters and believes that a 30-day time frame allows entities time to update their baseline configuration documentation. Similiarly, other commenters had issues with the 30-day time frame and the references to CIP-005 and CIP-007. These issues are no longer a concern, as the SDT has removed the reference to CIP-005 and CIP-007 in regards to the 30-day time frame.

Two commenters were concerned about 'triple', or 'double' jeopardy with CIP-005 and CIP-007. One commenter suggested a revision or removal of the references, while another suggested that the requirement be moved to CIP-005 or CIP-007. In consideration of their comment, the SDT has modified CIP-010-1 Requirement R1.3 accordingly. In response, references to CIP-005 and CIP-007 have been removed from the sub-part requirement language.

Requirement Part 1.4

Many comments stated that "High Impact BES Cyber Systems" should be removed from applicability in CIP-010-1 Requirement R1.4 since this requirement sub-part is repetitious with CIP-010-1 Requirement R1.5. While CIP-010-1 Requirement R1.4 has been modified due to comments from industry, the SDT disagrees that CIP-010 Requirement R1.4 is repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

A bevy of commenters believed that this requirement should include an exclusion for CIP Exceptional Circumstances. The SDT does not agree with this comment, as even after the CIP Exceptional Circumstance has happened, an entity should determine that controls were not adversely affected.

Several commenters suggested that guidance be added on cyber security controls. The SDT has taken their comment into consideration (in addition to other similar inquiries on cyber security controls) and added additional information on cyber security controls in CIP-010 guidance.

One commenter proposed the following language for this requirement part: "For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007, [do 1.4.2]." While the SDT considered this approach, the SDT believes the current requirement language is sufficient as is.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.1

One commenter suggested a language change of "determined" to "identified." The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed CIP-010-1 Requirement R1.4.1 where "could be impacted" is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where "could be impacted" is a remote possibility. Southern believed that documenting "what could be impacted" is not a reliability benefit, it's the verification that controls are not affected by a change. The SDT agrees with their recommended change, and the requirement language has been updated accordingly in Requirement R1 with: "implement, in a manner that identifies, assesses, and corrects deficiencies," to avoid the zero-defect audit enforcement concern.

Several commenters believed that CIP-010-1 Requirement R1.4.1 could result in the Responsible Entity declaring that no cyber security controls are expected to change and, thus, no testing is required. The SDT does not agree with this assessment, as the requirement requires documentation of what could be changed followed by verification that potentially impacted controls were not affected in CIP-010-1 Requirement R1.4.2.

Many commenters recommended the removal of Requirement R1.4.1. The concept is that an entity identifies all related controls that could be impacted based on all requirements in CIP-005 and CIP-007. Therefore, the SDT believes that by mentioning CIP-005 and CIP-007, there is no need for interpretations. In fulfilling the requirement, an entity must identify that a particular change impacts CIP-005-5 Requirement R1 or CIP-005-5 Requirement R1 and CIP-005-5 Requirement R2. If all requirements in CIP-005 and CIP-007 may be affected by a deviation to the existing baseline configuration, then this would be documented in accordance to CIP-010-1 Requirement R1.4.1. It should also be mentioned that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 Requirement R1.5. CIP-010-1 Requirement R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

CIP-010-1 Requirement Part 1.4, Sub-Part 1.4.2

One commenter mentioned that “BES Cyber Asset” should be replaced with “applicable Cyber Asset.” This comment was taken into consideration and the related requirement sub-part was modified. The phrase “BES Cyber System” was removed from the requirement sub-part for consistency.

Many commenters expressed concern with CIP-010-1 Requirement R1.4.2’s “availability” term. The SDT has modified the requirement language in consideration of these comments. The “available” term has been removed.

One commenter proposed that the word “determined” be changed to “identified.” The SDT disagrees with this proposed change and believes that the current language is sufficient as is.

One commenter believed the term “applicable” should be added for clarity. The SDT remarks that “applicable” is not required, as CIP-010 Requirement R1.4.2 points to CIP-010-1 Requirement R1.4.1, which ensures entities only look at the potentially impacted controls.

One commenter requested clarification of use of the term "required controls." The word required refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. While the SDT references all of CIP-005 and all of CIP-007, CIP-010-1 Requirement R1.4.1 requires entities to identify those controls in CIP-005 and CIP-007 that are potentially impacted. Therefore, CIP-010-1 Requirement R1.4.2 is only looking at the controls identified in CIP-010-1 Requirement R1.4.1.

One commenter proposed the addition of a time frame for how long an entity may take to make the verification required in CIP-010-1 Requirement R1.4.2. The SDT has taken this into consideration. The SDT also believes that the "identify, assess, and correct deficiencies" should provide aid in compliance concerns regarding this requirement.

CIP-010-1 Requirement Part 1.5, Sub-Part 1.5.1

Multiple commenters expressed concern with the language in CIP-010-1 Requirement R1.5.1. A few of the aforementioned organizations mentioned that the parenthetical expression in CIP-010-1 Requirement R1.5.1 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered. Other organizations recommended changing CIP-010-1 Requirement R1.5.1 language to: "testing cyber security controls, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. The SDT has reworded requirement language based on industry comment and hopes that the changes provide additional clarity. Alternatively, other organizations proposed the removal of the following language in CIP-010-1 Requirement R1.5.1: "…that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT disagrees with the comment, as documenting the differences between the test and production environment is a completely separate task compared to modeling the baseline configuration. Modeling the baseline configuration is an attempt to re-create the baseline configuration on a single asset, while documenting differences between the test and production environment would simulate the rest of the assets in that environment and how they function together. Other organizations were concerned that the revised language in the posted standard removed the possibility for a technical feasibility exception. The SDT does not agree, as old, legacy systems may not be available in a test environment and there may be no way to utilize a production environment where a test can be performed in a manner that minimizes adverse effects.

One commenter asked if this requirement interferes with CIP-010-1 Requirement R1.4 for High Impact Systems. There was a suggestion to remove the overlap in applicability of the two requirements and adding clarifying language as to

what is intended and required in CIP-010-1 Requirement R1.4 vs. CIP-010-1 Requirement R1.5. The SDT wishes to underscore that CIP-010-1 Requirement R1.4 is not repetitious with CIP-010-1 R1.5. CIP-010-1 R1.5 requires entities to test their baseline configuration changes in a test environment and document the results, while CIP-010-1 Requirement R1.4 requires entities to identify cyber security controls and then verify that these identified cyber security controls and system availability are not adversely affected after making the change.

One commenter requested clarification of use of the term: "required controls." The SDT responds by claiming that "required" refers to the cyber security controls in CIP-005 and CIP-007 that were applied based on asset identification in CIP-002. Additional information on cyber security controls were added in CIP-010-1 Guidelines for Requirement R1.

Several commenters expressed concern over the "where technically feasible" language. Alliant Energy proposed that: "where technically feasible" should be changed to "where test environments exist." One commenter wanted to know what the language pertained to. The SDT does not agree with the proposed modification. The language in the requirement allows for test environments to exist in a production environment where the test is performed in a manner that minimizes adverse effects. Also, it should be made clear that the exception language refers to both CIP-010-1 Requirement R1.5.1 and Requirement R1.5.2.

Requirement Part 1.5, Sub-Part 1.5.2

Some commenters believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." Another commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important.

SPP RE and City Utilities of Springfield, MO asked if CIP-010-1 Requirement R1.5.2 permits the documentation of a stand-alone test environment with identified differences from the production environment. The SDT concurs that the requirement language requests documentation of the differences between the test and production environment, if a test environment was used. If the differences did not change from change to change, then the same documentation would be included with each change package that is processed.

Requirement R1 VRFs

Based on numerous comments, the VRFs in Table of Compliance Elements now match the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirement R1 and Requirement R2.

Requirement R1 VSLs

There were two commenters who suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. The SDT will take this into consideration, as we apply the non-zero defect forward looking compliance process.

Two commenters suggested that "any" be changed to "one or more" in the High VSL for CIP-010-1 Requirement R1. The SDT has updated the VSL language per the comment's recommended change.

One commenter believed that the phrase "and to document those changes" in the first condition of the High VSL for CIP-010-1 Requirement R1 should be deleted, as it is duplicative of the second condition. The SDT has removed the second condition due to modification to the requirement language to remove reference to other CIP standards in CIP-010-1 Requirement R1.3.

Main Requirement R2

One commenter proposed revision of the Requirement R1 to: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

Requirement Part 2.1

Many comments were on the initial ballot posting language, as the successive ballot posting language is not understandable. The SDT has modified the requirement in consideration of their comment.

One commenter believed that double jeopardy exists with CIP-010-1 Requirement R1 and CIP-010-1 Requirement R2.1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under CIP-010-1 Requirement R1, not a separate requirement. The SDT disagrees with this assessment. CIP-010-1 Requirement

R2.1 does not create a double jeopardy situation with CIP-010-1 Requirement R1 since the violation would be in CIP-010-1 Requirement R1, not in CIP-010-1 Requirement R2.1. CIP-010-1 Requirement R2.1 requires entities to document and investigate detected unauthorized changes. If one of the unauthorized changes is due to a violation of CIP-010-1 Requirement R1, then the self-report would be on CIP-010-1 Requirement R1 and not on CIP-010-1 Requirement R2.1. However, based on the new "identifies, assesses, and corrects deficiencies" language, if an issue is detected, based on an entity's internal control processes, this would not be a self-report. Other commenters stated on CIP-010-1 Requirement R2 creating a situation where a need would exist to self-report. With the new requirement language of "identifies, assesses, and corrects deficiencies," a self-report would not be necessary.

Many commenters essentially mentioned concerns centered on technical feasibility language. Some of the aforementioned organizations requested that the term "continuous" be removed from requirement language; while others proposed language that would remove the technical feasibility exception. The SDT has modified the requirement language in consideration of these comments. One commenter further commented that the language should be revised in such a way that only devices that can monitor automatically should be included; otherwise, a technical feasibility exception should be allowed. The SDT has modified the language such that monitoring could be done manually or continuously depending on the device.

One commenter suggested a change to the following language: "Document changes tracked through the entity's change management program." The SDT does not agree with this approach and believes the language is sufficient as is. One commenter recommended a similar approach of modifying the language due to their desired removal of "baseline" term use.

Many commenters suggested a different time frame for monitoring. The suggestion called for a 90-day instead of 35-day time frame, while other commenters suggested an annual or quarterly time frame. The SDT believes that a 35-day time frame is sufficient for an "express acknowledgement."

One commenter believed that the requirement will be burdensome and nothing gained from it except a lot of TFE paperwork to track. The SDT disagrees with this comment, as the requirement was added based on FERC Order 706.

One commenter asked if no change is detected during a monitoring period, how an entity can demonstrate that "no change" occurred. The requirement language mentions that only detected unauthorized changes need to be documented and investigated. If there is no change, then this would not need to be documented.

Measures for Requirement Part 2.1
One commenter emphasized that the requirement requires monitoring for all changes, yet the measure mentions calls for investigation of any unauthorized changes. They believe that the requirement language should be changed to include "unauthorized" changes such that monitoring is only necessary for unauthorized changes. The SDT does not agree with this assessment and believes that the requirement language and measures are sufficient as is.

One commenter requested clarity on the phrase "record of investigation." "Record of investigation" would be some type of documentation that shows that a detected unauthorized change was documented and investigated accordingly.

Requirement R2 VRFs
Multiple commenters stated that the VRFs in the table of compliance elements now matches the VRF as identified at the requirements and measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R2 VSLs
Several commenters suggested that in corresponding to the proposed revisions to the requirement statement, the VSLs should be revised to: "severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention." The SDT will take this into consideration as we apply the "non-zero defect forward looking compliance process."

Two commenters believed that a new gradated VSL should be introduced due to time-period language added in the previous posting. The SDT has taken this comment into consideration. While gradated VSLs were not introduced, since the requirement language includes "… identify, assess, and correct deficiencies…", the VSLs have been updated. .

Requirement R3
One commenter proposed a revision to Requirement R1 to read: "Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations." The SDT has considered this approach in accordance with the FFT process. The following language has been added to requirement language: "identifies, assesses, and corrects deficiencies…"

A few commenters mentioned that the applicability between CIP-010-1 Requirements R3.3 and R3.4 differed. The SDT recognizes this difference and emphasizes that these are two different requirements and, hence, the applicability should be different.

One commenter asked if all Vulnerability Assessments under Requirement R3 must be performed prior to Version 5's Effective Date or whether entities have an additional year or three years from the effective date. The answer to NIPSCO's question can be found in the CIP Version 5 Implementation Plan. CIP-010-1 Requirements R3.1 and R3.2 must initially be complied with 12 months after the Effective Date of the CIP Version 5 standards.

One commenter asked why CIP-010-1 Requirement R3 does not always include Medium Impact in its scope. The SDT believes that the applicability as is can be considered sufficient. TRE also had concerns that the Requirement R3 does not include an annual vulnerability assessment. This is incorrect as CIP-010-1 Requirement R3.1 requires an annual vulnerability, while CIP-010-1 Requirement R3.2 requires a 36-month vulnerability assessment (for the applicable systems).

One commenter asked for clarity over the inclusion in applicability of Electronic Access Control or Monitoring Systems in CIP-010-1 Requirement R3. This requirement has the same applicability for these systems as in previous NERC CIP version. Therefore, the SDT believes that these systems should remain included in the applicability for CIP-010-1 Requirement R3.

One commenter asked if vulnerability assessments are required for every cyber asset or a sampling of cyber assets. Per applicable systems section, the vulnerability assessment is required for the systems listed.

Requirement Part 3.1

Commenters recommended that the requirement start with its purpose. The SDT disagrees with this comment, as the requirement language is consistent with other similar CIP V5 requirement language.

Many commenters proposed to reword Requirement R3.1 with the following language: "once each calendar year or a period not to exceed 15 calendar months between assessments." The SDT has taken these comments under consideration and is modifying the requirement sub-part language accordingly. One commenter proposed alternative language allowing an entity determined time frame. The SDT disagrees with this comment since the 15 calendar months' time frame is sufficient.

A few commenters believed that double jeopardy exists with reference to CIP-005, CIP-006, and CIP-007. The SDT does not agree, as if controls are not implemented correctly, then this would be a violation in the respective CIP standard, and not CIP-010-1.

Many commenters recommended that CIP-006 be removed from requirement language. The SDT agrees and has removed the reference to CIP-006.

Multiple commenters had concerns on what exactly constituted an active vulnerability assessment. The SDT points to guidance in CIP-010 on Requirement R3 in regards to recommended elements of an active vulnerability assessment. Also, other commenters asked if an active vulnerability assessment must be done for all systems or a representative sampling. Per the applicable systems section of the table for Requirement R3, the active vulnerability assessment must be done for all applicable systems.

One commenter requested clarification on whether an external vendor needs to perform the annual vulnerability assessment or can the Responsible Entity perform this task. The SDT provides enough flexibility in the requirement so that the RE can determine the solution that best meets its needs.

Several commenters believed that CIP-010-1 Requirement R3.1 is redundant with CIP-010-1 Requirement R1.3. The SDT does not agree, as CIP-010-1 Requirement R3.1 requires an annual vulnerability assessment, while CIP-010-1 Requirement R1.3 requires an update of the baseline configuration for a change that deviates from the existing baseline configuration.

Measure for Requirement Part 3.1
One commenter believed that reference to “individuals” in the first bulleted item needs to be removed. The SDT emphasizes that measures are only examples of evidence. However, the SDT has modified the measure language in consideration of the comment.

Requirement Part 3.2
Many commenters expressed concern with the language in CIP-010-1 R3.2. Another comment mentioned that the parenthetical expression in CIP-010-1 R3.2 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been

altered. Furthermore, the commenters recommended that this requirement start with its purpose. The SDT disagrees with these comments as the requirement language is consistent with other similar CIP Version 5 requirement language.

Multiple commenters asked for clarification on CIP-010-1 Requirement R3.2 in regards to this being a paper exercise. The requirement language mentions active vulnerability assessment. In response, please see the guidance section on additional details on an active vulnerability assessment.

Multiple commenters proposed the removal of the language: "that models the baseline configuration to ensure that required cyber security controls are not adversely affected" in CIP-010-1 Requirement R3.2, commenting that it is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. The SDT does not agree with this assessment. CIP-010-1, Requirement R3.2.1 requires performing an active vulnerability assessment in an environment that models the baseline configuration of the BES Cyber System in a production environment, while CIP-010-1 Requirement R3.2.2 requires documenting the results of testing, and if, a test environment was used, documenting the differences.

One commenter asked how is this requirement differs from CIP-007. The SDT remarks that CIP-010-1 Requirement R3.2 is related to completing a vulnerability assessment every three years to assess controls in CIP-007 (and CIP-005) are implemented correctly.

One commenter believed that the following language should be removed from the sub-requirement: "including a description of the measures used to account for any differences in operation between the test and production environments." One commenter stated that they do not understand the intent of requiring this type of documentation, as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. The SDT does not agree with this assessment and believes the documentation of the differences is important in establishing how the testing environments differ.

A few commenters asked if the assessment in CIP-010-1 Requirement R3.2 is in lieu of or in addition to the assessment required by CIP-010-1 Requirement R3.1 in the calendar year that the CIP-010-1 Requirement R3.2 assessment is conducted. The SDT believes that CIP-010-1 Requirement R3.2 is in lieu of CIP-010-1 Requirement R3.1 in the calendar year that CIP-010-1 Requirement R3.2 is conducted.

One commenter asked if CIP-006 is within scope of CIP-010-1 Requirement R3.2. The SDT has removed the reference to CIP-006 in CIP-010-1 Requirement R3.1, and is not a similar reference in CIP-010-1 Requirement R3.2.

One commenter proposed that the phrase: "where technically feasible" should be changed to "where test environments exist." The SDT does not agree with this modification since language in the requirement allows for "test environments" to exist in a production environment where the test is performed in a manner that minimizes adverse effects.

There was a comment mentioned that CIP-010-1 Requirement R3.2 requires assessments every three years, while CIP-007-3 Requirement R8 required vulnerability assessments annually. It was thought that we weakened the requirement; however, CIP-010-1 Requirement R3.1 requires an annual vulnerability and, therefore, the annual requirement in CIP-007-3 Requirement R8 was not weakened.

A commenter requested that associated electronic access control or monitoring systems and associated protected cyber assets should be added to the applicability for Requirement R3.2. For consistency in CIP-010-1, the SDT does not agree with the proposed change in applicability.

Requirement Part 3.3

One commenter believed it to be problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. The SDT acknowledges the concern, but emphasizes that an active vulnerability assessment is not required in the cases of a CIP Exceptional Circumstance or like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset.

One commenter believed that the term "active vulnerability assessment" is not defined. The SDT disagrees with this statement, as guidance is provided that aids in understanding an active vulnerability assessment. Furthermore, the commenter stated that since sufficient change management controls exist that an active vulnerability assessment is unnecessary. The SDT disagrees with this statement, as the configuration change management controls in CIP-010-1 Requirements R1 and R2 are in place for changes that deviate from the existing baseline configuration, while vulnerability assessments in CIP-010-1 Requirement R3 are for ensuring proper controls and detecting vulnerabilities.

One commenter mentioned that the parenthetical expression in CIP-010-1 Requirement R3.3 should be altered to no longer include parenthesis. This comment was taken into consideration and the related requirement sub-part was modified. The language in the requirement part has been altered.

Multiple commenters expressed concern around the language in CIP-010-1 Requirement R3.3. Some of the aforementioned organizations recommended that this requirement start with its purpose. Other organizations recommended a revision of the language. The SDT has taken these comments into consideration and modified the requirement language accordingly.

Multiple commenters suggested revisions to "prior to adding" language. One commenter proposed that instead of "prior to adding," that the requirement language should read: "before closing the change." Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

One commenter believed that the parenthetical explanation of a like replacement should be moved to guidance. The SDT disagrees with the proposed change and believes that the current language is sufficient based on other comments from industry.

Several commenters believed that CIP-010-1 Requirement R3.3 appears to be missing "and" after the parenthesis. Without the parenthetical, it should read "Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset..."

A couple commenters suggested that Physical Access Control Systems should be added in the applicable systems column. The SDT does not agree with their proposed change, as references to Physical Access Control Systems and CIP-006-1 have been removed throughout CIP-010-1.

One commenter expressed confusion around the use of the term: "new Cyber Asset." The commenter questioned if this term references a new Cyber Asset that is part of an existing Cyber System, or a new Cyber Asset per CIP-002. The SDT remarks that CIP-010-1 Requirement R3.3 is for new Cyber Assets with baseline configurations that do not currently exist. Therefore, a new Cyber Asset that is part of an existing Cyber System (and that has an existing baseline configuration) does not require an active vulnerability assessment per CIP-010-1 Requirement R3.3.

Several commenters believed that the language should be consistent among CIP-010-1 Requirements R3.1 through R3.3 in regards to vulnerability assessments. The SDT has modified the requirements accordingly in consideration of their comment.

A commenter asked if cyber assets can be placed in ESP before remediation of identified vulnerabilities. The SDT remarks that cyber assets can only be placed in ESP before remediation of identified vulnerabilities if a CIP Exceptional Circumstance exists or the cyber asset is a "like replacement."

CIP-010-1 Requirement Part 3.4

One commenter suggested that the term "if any" be added in CIP-010-1 Requirement R3.4 to denote the need to document the results of assessments that identified no vulnerabilities. The SDT disagrees as the language in CIP-010-1 Requirement R3.4 follows closely to the language in its previous instance in an earlier CIP standards version.

Many commenters expressed concern with the phrase: "remediate or mitigate vulnerabilities" and the related documentation. Another commenter proposed to replace "remediate or mitigate vulnerabilities" with "implement lessons learned (if any)" for consistency with other standards and eliminate extra documentation tracking requirements. The SDT developed this requirement language directly from the previous CIP versions. The concept is that an entity must document how they plan to remediate or mitigate identified vulnerabilities. CIP-010-1 Requirement R3 becomes an internal controls requirement to ensure that cyber security controls are properly implemented. While other commenters asked if it is the intent that identified vulnerabilities would not constitute violations of requirements they are found against. It is not the SDT's intent that an identified vulnerability would not constitute a violation of other requirements. While CIP-010 would not be violated, the respective CIP-005 or CIP-007 standard may be violated. The SDT does believe that the self-report mitigation plan could be used as the action plan for Requirement R3.4.

Several entities believed that the deadline for documenting the results of the assessment and the action plan should be specified. They suggested a 30-day limit. Also, they suggested including levels of gradation for not meeting the 30-day limit. One commenter took a different approach and recommended that "planned date" be changed to "estimated time frame." The SDT believes that the requirement language is sufficient as is.

Several commenters believed that more specificity should be added around the term “assessments” in CIP-010-1 Requirement R3.4. The SDT has modified the language in consideration of these comments and the text: “conducted pursuant to Parts 3.1, 3.2, and 3.3” was added to the requirement language.

One commenter asked for clarity in regards to the phrase “planned date of completing the action plan.” Is this the completion of the formulation of the plan or the completion of the tasks within the plan? The SDT articulates that the planned date of completing the action plan is related to the completion of the tasks within the plan.

Requirement R3 VRFs

There were multiple comments on VRFs, and the VRFs in Table of Compliance Elements now matches the VRF as identified at the Requirements and Measures section of the standard. This modification is for both CIP-010-1 Requirements R1 and R2.

Requirement R3 VSLs

Several commenters believed that corresponding to the proposed revisions to the requirement statement that the VSLs should be revised to read: “severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.” The SDT has taken this comment into consideration as we applied the “identify, assess, and correct” approach; however, that language should not be included here. The reasoning behind this decision is due to the CIP-010-1 R3 Requirement’s indirect (mentioned in R3 Guidance) reference to CIP-005 and CIP-007. The related language would relate to the timely performance of completing a vulnerability assessment instead of identifying and correcting deficiencies which may be a part of the related CIP-005 and CIP-007 langauge (CIP-005 does not include this language in its requirements).

Several commenters proposed that the third condition in Severe VSL have the word “or” instead of “and.” The SDT has modified the language in response to their comment.

One commenter believed that the VSL does not address the 36-month timeline in CIP-010-1 Requirement R3.2. Furthermore, the commenter proposed additional language to address this timeline. The SDT has taken this comment into consideration and modified the VSL language accordingly.

QUESTION C15 – CIP-011-5:

If you disagree with the changes made in CIP-011-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:
Based on stakeholder comments, there were many global comments that related not only to CIP-011, but to all of the CIP standards.

Annual Requirements
Many commenters objected to the posted language referencing annual requirements. Several suggested alternative ways to express the frequency for an annual requirement. The SDT considered all of the recommendations and decided use the phrase "at least once every 15 calendar months" (or similar) to express the frequency for annual requirements.

Use of the phrase "but not limited to" in measures language
The SDT received many comments objecting to the phrase "but not limited to" within the measures. Some comments suggested removal of the term; others recommended a default to the use of the word "or," while others suggested the use of the word "and." Commenters believed that using the "but not limited to" language creates confusion about whether the specified measures are necessary or sufficient. The SDT has considered this issue carefully. The SDT has modified the language to "examples of acceptable evidence include, but are not limited to." The phrase "but not limited to" is designed to be of benefit to the Responsible Entity, not be a back door "gotcha" for auditors. Use of the phrase allows the entity flexibility in the type of evidence they are able to provide both now and in the future.

Applicability Column Title
The length of the applicability column title caused confusion about the systems/assets that are within scope for some entities. Several commenters suggested shortening the column heading to "applicability." The SDT recalls that the title of the column as previously posted was in response to comments from the first posting. SDT has renamed the column "applicable systems."

The SDT received many comments stating that: "Medium Impact BES Cyber Systems should be limited to Medium Impact BES Cyber Systems with External Routable Connectivity to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP Version 4 standards." A main goal of the SDT is to implement the FERC directives in Order 706 and Order 761. Order 761 states that FERC: "…supports the elimination of the blanket

exemption for non-routable connected cyber systems…continued blanket exemption in Version 5 would not adequately address risk." The SDT has considered each requirement concerning handling the exemption for non-routable connections. The SDT does not agree that in CIP-011 the scope should be limited to only BES Cyber Systems with External Routable Connectivity, as recommended in some comments.

Many commenters requested the removal of all references to systems and assets in requirements and that the SDT rely on the applicability column only to specify applicability. The SDT agrees with this recommendation. Wherever possible, the assets in scope will be indicated only in the applicability column. Several commenters suggested that the SDT remove all references to applicable assets in requirements and rely on the applicability column only to specify the Cyber Assets that are in scope. The SDT agrees. Wherever possible, the requirements have been streamlined to only reference applicable Cyber Assets within the applicability column.

Some commenters stated that the rationale for CIP-011 Requirement R1 was incomplete as originally posted. On May 8, 2012, NERC was alerted that the text contained in the rationale box for Requirement R1 of CIP-011-1 appeared to be incomplete. NERC corrected this by issuing revised language that modified the text box size to display all of the text.

Some commenters recommended that entities should define their own info protection program. They suggested that compliance would be evaluated based on how the entity complied with their defined programs. The SDT discussed this comment, but disagrees. The SDT believes it would be doing the industry a disservice to leave the process completely up to the entity. As part of its change, the SDT seeks to clarify what is required to meet compliance. The SDT believes that if the requirements are not defined or entity defined, NERC will be forced to issue Compliance Application Notices in the future to provide clarity, and auditors will be forced to inject their own audit measurements. In the interest of providing clarity, the SDT believes it is important to provide a consistent threshold for compliance.

The SDT received comments asking that the team revert to legacy language used in previous versions of the CIP standards (V1 and V3). SDT considered this request, but believes that many entities have made good suggestions, which improve legacy language. Legacy language will be utilized in all cases where it is appropriate for the purposes of minimizing changes that the registered entities must make to their ongoing programs.

CIP-011 Requirement R1 calls for each Responsible Entity to implement an information protection program that includes applicable items, and Requirement R1.1 requires methods to identify such information. Many entities commented that Requirement R1.1 was too vague. In fact, several entities indicated they were confused as to whether the requirement

called for determining what information should be protected or if the requirement mandated labeling of the information. Some entities asked if specific classification was required. A few entities suggested that a specific classification, such as "confidential," should be included in the requirement. The SDT has considered this but does not believe it is appropriate to dictate a specific classification, such as "confidential." Some entities may use other classifications such as "CIP-Confidential," "Non-Public," "Highly Confidential," or many other designations. It is not the intent of the SDT to force all Registered Entities to modify their compliance documentation by mandating specific classifications. This initial part of the information protection program simply requires that the information in scope and to be protected is identified in some manner. Specific classification of information may be used as a method for identification, but is not specifically required. One commenter provided a specific recommendation to clarify that the information to be identified is that which is explained in the definition of BES Cyber System Information. The SDT agrees with this comment. The SDT is also responsive to industry comments and has enhanced the measures section of Requirement R1.

Some entities pointed out that the word "implemented" is unnecessary in the Requirement R1.1 requirement because it is contained in the overall Requirement R1 requirement language. They asked that the word "implement" be removed from Requirement R1.1 because it was redundant. Other entities stated that documentation is for measures or evidence, and the word "documented" should be removed from Requirement R1.1 requirement. The SDT has removed both "implemented" and "documented" from the requirement language. The term documented has been moved to the measures section.

There were additional comments related to the measures for Requirement R1.1. Some commenters asked how a repository could be a measure, and others asked for additional clarity. A repository could be a measure if the entity designated the repository or a section of the repository as the location for identifying and housing BES Cyber System Information and explained the protections afforded by the repository in the entity's Information Protection Program. It would be up to the entity to explain in their information protection program how the repository was used to identify their BES Cyber System Information.

In CIP-011 Requirement R1.2, many commenters again asked that additional clarification be added to the requirement concerning procedures for handling of BES Cyber System Information. The SDT agrees and has modified the requirement to clarify that handling procedures required are those which explain how the BES Cyber System Information is protected and secured.

Several comments asked for additional specifics concerning several topics regarding BES Cyber System Information; including transit, handling, and transmittal. The SDT agrees with this. The guidance section has been greatly expanded to address the topics requested.

Several entities desired additional specifics concerning the measures for Requirement R1.2. One entity commented: "This measure does not specify what records could be used …would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?" The SDT disagrees that it would serve the industry to mandate this level of specifics within CIP-011. It is the SDTs intent that the entities document their information protection program and associated procedures in accordance with the CIP-011 requirements, and that the entity maintains records indicating that BES Cyber System Information is handled in a manner consistent with the entity's documented program and associated procedures. A measure has been added which specifies this intent.

There were several comments requesting that the SDT address third party handling of BES Cyber System Information. The SDT agrees with this comment. Additional information has been added to guidance to cover this topic.

There were comments asking for more specifics concerning the topics of transit, handling, transmittal, distribution, physical access, purge, use, and disposal. The guidance section has been significantly enhanced to address the topics for which additional direction is warranted.

Some commenters recommended including procedures for reuse and disposal within Requirement R1. The SDT does not agree. SDT believes that the topic of reuse and disposal is complex and requires the specifics currently afforded the topic as specified in Requirement R2. If the topic was included in the Requirement R1 procedures, it could result in double jeopardy during audits, as auditors review compliance with Requirement R1 procedures and Requirement R2 handling during reuse and disposal.

Commenters stated that the reference to prior version under Requirement R1.2 refers to CIP-003-3, Requirement R5.3. They recommended that the reference be moved to Requirement R1.3. The SDT agrees.

The SDT received many comments related to Requirement R1.3. Many commenters recommended that the team specify that deficiencies found in the annual assessment should not be considered violations or potential violations. Some commenters asked that the SDT specify which deficiencies would be considered violations and which would not be considered violations. Commenters asked that the word "deficiencies" be changed to "lessons learned" or "flaws." The

SDT notes that the word “deficiencies” is appropriate because a deficiency notes there is a lack of completeness or insufficiency exists.

Some asked that the entire requirement be handled under the NERC FFT program and eliminated from the requirements. It is not up to the SDT to make the determination as to what is and what is not a violation. The SDT sought guidance from NERC and regional audit staff. The audit staff advised that some deficiencies could be seen as self-reportable violations or potential violations during audit if the entity failed to adhere to one of the specified sub-requirements. Other deficiencies might simply be process improvements or opportunities for improvements that do not violate any BES Cyber System Information sub-requirement from CIP-011. Further, the requirement calls for a periodic “assessment,” and such “assessment” may reveal things that went well in addition to things that could be improved. After considering industry comments and consulting with audit and NERC staff, the requirement will be handled under the Paragraph 81 project from the FERC Order on the find, fix, track and report process.

Some commenters did not like the grouping of all access control requirements within CIP 004. They asked that the requirement parts dealing with access to information be moved into CIP-011. This was discussed among the SDT. It was decided that the majority of entities favored the grouping of all access control within CIP 004. For consistency and in response to many previous comments, all access control requirements have been grouped into CIP 004. The requirement parts dealing with access control for BES Cyber System Information have, therefore, not been moved into CIP-011.

Some commenters asked where specifically the process covering reuse and disposal is required. Requirement R2 states: “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal.” Therefore, Requirement R2 requires the entity to define their process concerning the topics within Requirement R2.

The SDT received comments questioning a discrepancy between the types of systems referenced in the definition of BES Cyber System Information vs. the applicability column for Requirement R2. Associated Protected Cyber Assets is included in the applicability column, but is not specifically referenced in the definition. The SDT’s intent is that if BES Cyber System Information as defined in the standard exists in the data storage media of applicable Cyber Assets, then Requirement R2 applies.

One commenter pointed out that the component obligations under CIP-011-1 are not clear and that the table headers under Requirement R2 may be adding to the confusion, as they are different for Requirements R2.1 and for R2.2. The SDT agrees and has corrected the table headers so that they are consistent within Requirement R2.

The second paragraph in Requirements R2.1 and R2.2 that deal with removal of the device from the PSP generated many comments. Some commenters asked that the language concerning removal from the PSP be clarified. Others asked that the language be moved to a separate part. Others stated that the language adds no value and asked that the language concerning removal from the PSP be deleted from the requirement part altogether. A few commenters suggested simplified language, and such comments were very much appreciated. The SDT has decided to remove from the requirement language dealing with removal from the PSP. The SDT will address the topic of removal from the PSP within the guidance section. The SDT made corresponding changes to the measures section.

Many commenters objected to use of the term “chain of custody” in Requirements R2.1 and R2.2. They stated that this is a legal term, and they believe it is not appropriate in the CIP standards. Others commented that the intended use of the term “who has possession,” as used in the requirement, was unclear. The SDT has decided to remove the entire second paragraph from Requirements R2.1 and R2.2, including the reference to “chain of custody.” The SDT made corresponding changes to the measures section and any reference to terms such as “chain of custody” has been removed from the measures section, as well.

Some commenters recommended combining Requirements R2.1 and R2.2 into one requirement part. The SDT disagrees with this recommendation. SDT believes there are sufficient differences in the handling of release for reuse versus disposal to warrant retaining both Requirement R2.1 and Requirement R2.2.

Within the Requirement R2.1 language, some commenters asked for additional clarity concerning the exception, which provides for reuse within other high impact or medium impact BES Cyber Systems. The SDT agrees with this comment and has added additional clarity to the guidance language specifying that the re-use exception applies to re-use in other systems that are identified in the applicable systems column as protections will continue after re-use.

The SDT received comments asking that “BES” be inserted in front of “Cyber Assets” within the reference to “applicable Cyber Assets that contain BES Cyber System Information...” within Requirements R2.1 and R2.2. The SDT disagrees with this direction. The requirement parts are applicable to Associated Physical Access Control Systems, Associated Electronic

Access Control or Monitoring Systems, and Associated Protected Cyber Assets. Therefore, the scope of Cyber Assets which may contain BES Cyber System Information is larger than the suggested term "BES Cyber Assets."

The SDT received at least one comment stating that it was unclear if Requirement R2.2 meant the storage media within the Cyber Asset, or if it also includes backup media. The requirement states: "Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media." The SDT's intent is that the scope includes the Cyber Asset data storage media. The scope of this requirement is not far reaching to include all possible locations of downstream information, such as backup copies outside the Cyber Asset. However, such copies of BES Cyber System Information would be governed by Requirement R1.

Some entities also asked for additional specifics concerning the actions a Responsible Entity shall take to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. One commenter questioned whether an attestation was specifically mandated. An attestation is not required by the standard. It is not the intent of the SDT to mandate specific actions within the requirements. However, the guidance section has been greatly expanded with guidance taken from NIST SP800-88, which provides additional assistance to entities.

One entity stated that it is not clear if requirement parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. The SDT considered this question and believes that the answer is: Yes, such actions would be permitted. The requirement calls for the entity to "take action to prevent unauthorized retrieval." This provides flexibility for the entity. As long as the entity documented the actions that they undertook; i.e., removing the media, securing the media, sanitizing the media in accord with the requirements, such action should be permitted.

SDT received the following comment: requirement part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contain BES Cyber System Information (i.e., network diagram). The second sentence appears to pertain to Cyber Assets within an ESP. There were other commenters asking for clarity concerning the storage media and the targets for sanitation in Requirement R2. Requirement R2 applies to any information within the Cyber Asset data storage media that meets the definition of BES Cyber System Information.

A few commenters stated that the standard needs to track the media and not necessarily the Cyber Asset the media is associated with. The SDT agrees with this comment. The Requirement R2 language has been modified to include the reference to "data storage media."

VSLs and VRFs

The SDT received at least one comment asking that the VRF for Requirement R1 be lowered. The SDT disagrees with the industry comment. The VRF for Requirement R1 is Medium in keeping with the FERC approved current VRF for this requirement. The VRF for Requirement R2 is already lower.

One commenter asked that the SDT add the "part" reference to the VSL so that the reader could easily understand the requirement number to which the VSL referred. The SDT agrees with this comment, and added the references to the VSL's.

Multiple commenters objected to the "zero defect" approach to VSL's for Requirement R2. The SDT agrees. The previously posted Requirement R2 VSLs have been modified to be less "device" specific. In the future, there will be additional emphasis on the entity providing good processes and security controls.

One commenter provided specific language for VSL's. Corresponding to recommendations that had been made concerning requirements, they asked that the VSLs should be revised to: Severe-not implemented, Higher-not measuring to detect, Moderate-not correcting detected flaws, Lower-not considering prevention. However, the requirement does not address prevention, and the VSLs must correspond to the requirements.

NERC will be sharing additional information on VRFs and VSLs in keeping with NERC's implementation of the FFT program.

Questions with Votes Only:

CIP-008, CIP-009, CIP-010 and CIP-011 Questions: Question 1

1. **CIP-008-5 R1 states "Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable items in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?**

Organization	Yes or No
Northeast Power Coordinating Council	No
Duke Energy	No
NESCOR/NESCO	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No

Organization	Yes or No
NIPSCO	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No

Organization	Yes or No
Kansas City Power & Light	No
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes

Organization	Yes or No
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes

Organization	Yes or No
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
PJM Interconnection	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes

Organization	Yes or No
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

2. CIP-008-5 R2 states "Each Responsible Entity shall implement its documented Cyber Security Incident response plan(s) to collectively include each of the applicable items in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Dairyland Power Cooperative	No

Organization	Yes or No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes

Organization	Yes or No
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes

Organization	Yes or No
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Springfield Utility Board	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
California Independent System Operator	Yes

3. CIP-008-5 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
PNM Resources	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Hydro One	No
Lakeland Electric	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
MRO NSRF	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review	Yes

Organization	Yes or No
Committee	
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes

Organization	Yes or No
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes

Organization	Yes or No
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Pacific Gas and Electric Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes

5. CIP-009-5 R1 states "Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in CIP-009-5 Table R1 – Recovery Plan Specifications." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No

Organization	Yes or No
Florida Municipal Power Agency	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Lakeland Electric	No

Organization	Yes or No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
Massachusetts Municipal Wholesale Electric Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
Utility Services Inc.	No

Organization	Yes or No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Farmington Electric Utility System	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Pepco Holdings Inc & Affiliates	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces	Yes

Organization	Yes or No
Corporation	
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes

Organization	Yes or No
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes
Portland General Electric	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

6. CIP-009-5 R2 states "Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in CIP-009-5 Table R2 – Recovery Plan Implementation and Testing." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
MRO NSRF	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
Puget Sound Energy, Inc.	No
PNM Resources	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
Lincoln Electric System	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Alliant Energy	No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes

Organization	Yes or No
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
CenterPoint Energy	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes

Organization	Yes or No
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Oncor Electric Delivery Company LLC	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes

Organization	Yes or No
Utility Services Inc.	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes

7. CIP-009-5 R3 states "Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Summary Consideration:

Organization	Yes or No
NRG Energy Companies	No
PPL Corporation NERC Registered Affiliates	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
SMUD & BANC	No
PNM Resources	No
Arizona Public Service Company	No
Progress Energy	No
Hydro One	No
Tampa Electric Company	No

Organization	Yes or No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Oncor Electric Delivery Company LLC	No
CenterPoint Energy	No
Xcel Energy	No
New York Power Authority	No
MidAmerican Energy Company	No
PJM Interconnection	No
ISO New England Inc.	No
ACES Power Marketing	No
Puget Sound Energy, Inc.	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
Brazos Electric Power Cooperative	No
IRC Standards Review Committee	Yes
The united illuminating Company	Yes
Lakeland Electric	Yes
Southern California Edison Company	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Northeast Utilities	Yes
Portland General Electric	Yes
MRO NSRF	Yes
NESCOR/NESCO	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
Comment Development SME list	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Dairyland Power Cooperative	Yes
Tri-State G&T - Transmission	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes
MEAG Power	Yes
Utility Services Inc.	Yes

Organization	Yes or No
Alliant Energy	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Kansas City Power & Light	Yes
California Independent System Operator	Yes
Luminant	
American Transmission Company, LLC	
Avista	

9. CIP-010-1 R1 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R1 – Configuration Change Management." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
FirstEnergy	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No

Organization	Yes or No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Lower Colorado River Authority	No
LCRA Transmission Serivces Corporation	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No

Organization	Yes or No
MidAmerican Energy Company	No
NV Energy	No
Massachusetts Municipal Wholesale Electric Company	No
Detroit Edison Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No

Organization	Yes or No
Utility Services Inc.	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Exelon Corporation and its affiliates	No
Tucson Electric Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric	Yes

Organization	Yes or No
Cooperative, Inc. (NCR01177, JRO00088)	
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

10. CIP-010-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R2 – Configuration Monitoring." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
SMUD & BANC	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Western Area Power Administration	No

Organization	Yes or No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
ATCO Electric	No
Hydro-Quebec TransEnergie	No
Lincoln Electric System	No
The united illuminating Company	No
Bonneville Power Administration	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
Detroit Edison Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No
NYISO	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No

Organization	Yes or No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Texas RE NERC Standards Review Subcommittee	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes

Organization	Yes or No
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Serivces Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
Texas Reliability Entity	Yes
City of Austin dba Austin Energy	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Exelon Corporation and its affiliates	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

11. CIP-010-1 R3 states "Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable items in CIP-010-1 Table R3– Vulnerability Assessments." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
MRO NSRF	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
IRC Standards Review Committee	No
PNM Resources	No
Southern Company Services, Inc.	No

Organization	Yes or No
Western Area Power Administration	No
Dairyland Power Cooperative	No
Progress Energy	No
CenterPoint Energy	No
Hydro One	No
Central Hudson Gas & Electric Corporation	No
Independent Electricity System Operator	No
Hydro-Quebec TransEnergie	No
Consumers Energy Company	No
Lincoln Electric System	No
The united illuminating Company	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy	No

Organization	Yes or No
Company	
The Empire District Electric Company	No
NextEra Energy, Inc.	No
Texas Reliability Entity	No
Nebraska Public Power District	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Alliant Energy	No
Springfield Utility Board	No

Organization	Yes or No
NYISO	No
Exelon Corporation and its affiliates	No
Los Angeles Department of Water and Power	No
Kansas City Power & Light	No
California Independent System Operator	No
PPL Corporation NERC Registered Affiliates	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison Company	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Niagara Mohawk (dba National Grid)	Yes

Organization	Yes or No
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
PSEG	Yes
Liberty Electric Power, LLC	Yes
MEAG Power	Yes

Organization	Yes or No
Portland General Electric	Yes
Utility Services Inc.	Yes
Pacific Gas and Electric Company	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes

13. CIP-011-1 R1 states "Each Responsible Entity shall implement an information protection program that includes each of the applicable items in CIP-011-1 Table R1 – Information Protection." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NRG Energy Companies	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
PNM Resources	No
National Rural Electric Cooperative Association (NRECA)	No
Progress Energy	No
CenterPoint Energy	No

Organization	Yes or No
Tri-State G&T - Transmission	No
Xcel Energy	No
Snohomish County PUD	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
NextEra Energy, Inc.	No
PSEG	No
Liberty Electric Power, LLC	No
Texas Reliability Entity	No
PJM Interconnection	No
Oncor Electric Delivery Company LLC	No
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No

Organization	Yes or No
Wisconsin Electric Power Company	No
Exelon Corporation and its affiliates	No
Deseret Power	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
ACES Power Marketing	Yes

Organization	Yes or No
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes

Organization	Yes or No
Central Hudson Gas & Electric Corporation	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
The united illuminating Company	Yes
Turlock Irrigation District	Yes
Bonneville Power	Yes

Organization	Yes or No
Administration	
Lakeland Electric	Yes
Tampa Electric Company	Yes
New York Power Authority	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
Northeast Utilities	Yes
Nebraska Public Power District	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes

Organization	Yes or No
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Farmington Electric Utility System	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes
Brazos Electric Power Cooperative	Yes
California Independent System Operator	Yes

14. CIP-011-1 R2 states "Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal." The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
Duke Energy	No
NESCOR/NESCO	No
Dominion	No
Texas RE NERC Standards Review Subcommittee	No
ACES Power Marketing	No
PNM Resources	No
Southern Company Services, Inc.	No
Progress Energy	No
Tri-State G&T - Transmission	No

Organization	Yes or No
Hydro One	No
Independent Electricity System Operator	No
The united illuminating Company	No
Xcel Energy	No
Tampa Electric Company	No
New York Power Authority	No
MidAmerican Energy Company	No
The Empire District Electric Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power, LLC	No
PJM Interconnection	No
ISO New England Inc.	No
Oncor Electric Delivery	No

Organization	Yes or No
Company LLC	
City of Austin dba Austin Energy	No
City Utilities of Springfield, MO	No
Wisconsin Electric Power Company	No
Pacific Gas and Electric Company	No
NYISO	No
Exelon Corporation and its affiliates	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
NRG Energy Companies	Yes
PPL Corporation NERC Registered Affiliates	Yes

Organization	Yes or No
MRO NSRF	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
Pepco Holdings Inc & Affiliates	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Puget Sound Energy, Inc.	Yes
Comment Development SME list	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes

Organization	Yes or No
Western Area Power Administration	Yes
Southern California Edison Company	Yes
Dairyland Power Cooperative	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Central Hudson Gas & Electric Corporation	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Serivces Corporation	Yes
Hydro-Quebec TransEnergie	Yes
Consumers Energy Company	Yes
Lincoln Electric System	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Detroit Edison Company	Yes
Tennessee Valley Authority	Yes
Northeast Utilities	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Nebraska Public Power District	Yes

Organization	Yes or No
MEAG Power	Yes
Portland General Electric	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
Springfield Utility Board	Yes
Farmington Electric Utility System	Yes
Deseret Power	Yes
Central Lincoln	Yes
Tucson Electric Power	Yes
Cowlitz County PUD	Yes
Los Angeles Department of Water and Power	Yes

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Cyber Security Order 706 Version 5 CIP Standards
Comment Form D
Definitions and Implementation Plans

The Cyber Security Order 706 Drafting Team thanks all commenters who submitted comments on the CIP Version 5 standards. These standards were posted for a 40-day public comment period from April 12, 2012 through May 21, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 119 sets of comments, including comments from approximately 270 different people from approximately 171 companies representing 9 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.	Greg Campoli	New York Independent System Operator	NPCC	2
3.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
4.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1
5.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
6.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
7.	Kathleen Goodman	ISO - New England	NPCC	2
8.	David Kiguel	Hydro One Networks Inc.	NPCC	1
9.	Michael Lombardi	Northeast Utilities	NPCC	1
10.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Bruce Metruck	New York Power Authority	NPCC	6
12.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
13.	Robert Pellegrini	The United Illuminating Company	NPCC	1
14.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
15.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
16.	Brian Robinson	Utility Services	NPCC	8
17.	Michael Jones	National Grid	NPCC	1
18.	Michael Schiavone	National Grid	NPCC	1
19.	Wayne Sipperly	New York Power Authority	NPCC	5
20.	Tina Teng	Independent Electricity System Operator	NPCC	2
21.	Don Weaver	New Brunswick System Operator	NPCC	2
22.	Ben Wu	Orange and Rockland Utilities	NPCC	1
23.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3
24.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5

2.	Group	Annabelle Lee	NESCOR/NESCO										

	Additional Member	Additional Organization	Region	Segment Selection
1.	Andrew Wright	N-Dimension Solutions		
2.	Chan Park	N-Dimension Solutions		
3.	Dan Widger	N-Dimension Solutions		
4.	Stacy Bresler	NESCO		
5.	Carol Muehrcke	Adventium Enterprises		
6.	Josh Axelrod	Ernst & Young		
7.	Glen Chason	EPRI		
8.	Elizabeth Sisley	Calm Sunrise Consulting		

3.	Group	Jason Marshall	ACES Power Marketing						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Ringhausen	Old Dominion Electric Cooperative	RFC	3, 4
2.	Susan Sosbe	Wabash Valley Power Association	RFC	3
3.	Megan Wagner	Sunflower Electric Power Corporation	SPP	1
4.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
5.	Erin Woods	East Kentucky Power Cooperative	SERC	1, 3, 5

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Shari Heino	Brazos Electric Power Cooperative	ERCOT 1										
4.	Group	Stephen Berger	PPL Corporation NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Annette Bannon	PPL Generation, LLC on Behalf of its NERC Registered Entities	RFC	5
2.			WECC	5
3.	Mark Heimbach	PPL EnergyPlus, LLC	MRO	6
4.			NPCC	6
5.			SERC	6
6.			SPP	6
7.			RFC	6
8.			WECC	6
9.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
10.	Brent Ingebrigtson	LG&E and KU Services Company	SERC	3

5.	Group	Patricia Robertson	BC Hydro	X	X	X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Venkatarmakrishnan Vinnakota	BC Hydro	WECC	2
2.	Pat G. Harrington	BC Hydro	WECC	3
3.	Clement Ma	BC Hydro	WECC	5

6.	Group	Christine Hasha	IRC Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Thompson	AESO	WECC	2
2.	Steve Myers	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Marie Knox	MISO	RFC	2
5.	Stephanie Monzon	PJM	RFC	2
6.	Charles Yeung	SPP	SPP	2

7.	Group	Brenda Hampton	Texas RE NERC Standards Review Subcommittee						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6

8.	Group	Emily Pennel	Southwest Power Pool Regional Entity									X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rayburn Country Electric Cooperative		SPP	
2.	Empire District Electric		SPP	1
3.	City Utilities of Springfield		SPP	4
4.	Westar Energy		SPP	1, 3, 5, 6
5.	Cleco Power		SPP	1, 3, 5, 6

9.	Group	Alan Johnson	NRG Companies					X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Rick Keetch	NRG Power Marketing LLC	ERCOT	3
2.	Richard Comeaux	Lagen	SERC	4

10.	Group	Greg Rowland	Duke Energy	X		X		X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Ed Ernst	Duke Energy	SERC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

11.	Group	Ron Sporseen	PNGC Comment Group	X		X	X				X		

	Additional Member	Additional Organization	Region	Segment Selection
1.	Joe Jarvis	Blachly-Lane Electric Cooperative	WECC	3
2.	Dave Markham	Central Electric Cooperative	WECC	3
3.	Dave Hagen	Clearwater Power Company	WECC	3
4.	Roman Gillen	Consumers Power Inc.	WECC	1, 3
5.	Roger Meader	Coos-Curry Electric Cooperative	WECC	3
6.	Bryan Case	Fall River Electric Cooperative	WECC	3

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
7.	Rick Crinklaw	Lane Electric Cooperative	WECC 3										
8.	Annie Terracciano	Northern Lights Inc.	WECC 3										
9.	Aleka Scott	PNGC	WECC 4										
10.	Heber Carpenter	Raft River Electric Cooperative	WECC 3										
11.	Steve Eldrige	Umatilla Electric Cooperative	WECC 1, 3										
12.	Marc Farmer	West Oregon Electric Cooperative	WECC 4										
13.	Margaret Ryan	PNGC	WECC 8										
12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sam Ciccone	FE	RFC	
2.	Cindy A. Sheehan	FE	RFC	
3.	David A. Griffin	FE	RFC	
4.	Larry A Raczkowski	FE	RFC	
5.	Kenneth J. Dresner	FE	RFC	
6.	Michael T Bailey	FE	RFC	
7.	Peter J. Buerling	FE	RFC	
8.	Troy K. Rhoades	FE	RFC	
9.	Heather Herling	FE	RFC	
10.	Mark A. Koziel	FE	RFC	

13.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		MRO	5
2.	Mike Garton		NPCC	5, 6
3.	Louis Slade		RFC	5
4.	Michael Crowley		SERC	1, 3, 5, 6

14.	Group	David Dockery, NERC Reliability Compliance Coordinator, AECI	Associated Electric Cooperative, Inc. (JRO00088, NCR01177)	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	M & A Electric Power Cooperative	SERC	1, 3	
4.	Northeast Missouri Electric Power Cooperative	SERC	1, 3	
5.	N.W. Electric Power Cooperative, Inc.	SERC	1, 3	
6.	Sho-Me Power Electric Cooperative	SERC	1, 3	

15.	Group	Guy Andrews	Family Of Companies (FOC) including OPC, GTC & GSOC			X	X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Oglethorpe Power Corporation		SERC	5
2.	Georgia Transmission Corporation		SERC	1

16.	Group	Will Smith	MRO NSRF	X	X	X	X	X	X				X

	Additional Member	Additional Organization	Region	Segment Selection
1.	MAHMOOD SAFI	OPPD	MRO	1, 3, 5, 6
2.	CHUCK LAWERENCE	ATC	MRO	1
3.	TOM WEBB	WPS	MRO	3, 4, 5, 6
4.	JODI JENSON	WAPA	MRO	1, 6
5.	KEN GOLDSMITH	ALTW	MRO	4
6.	DAVE RUDOLPH	BEPC	MRO	1, 3, 5, 6
7.	JOE DEPOORTER	MGE	MRO	3, 4, 5, 6
8.	SCOTT NICKELS	RPU	MRO	4
9.	TERRY HARBOUR	MEC	MRO	1, 3, 5, 6
10.	MARIE KNOX	MISO	MRO	2
11.	LEE KITTELSON	OTP	MRO	1, 3, 4, 5
12.	SCOTT BOS	MPW	MRO	6, 1, 3, 5
13.	TONY EDDLEMAN	NPPD	MRO	1, 3, 5
14.	THERESA ALLARD	MPC	MRO	1, 3, 5, 6

17.	Group	David Batz	Edison Electric Institute	X				X					
www.eei.org for Member listing												
18.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Timothy Beyrle	City of New Smyrna Beach	FRCC	4
2.	James Howard	Lakeland Electric	FRCC	3

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Joe Stonecipher	Beaches Energy Services	FRCC	1
6.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4
7.	Randy Hahn	Ocala Utility Services	FRCC	3

19.	Group	Joseph DePoorter	Madison Gas and Electric Company			X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Darl Shimko	MGE	MRO	3
2.	Joseph DePoorter	MGE	MRO	4
3.	Steve Schultz	MGE	MRO	5
4.	Jeff Keebler	MGE	MRO	6

20.	Group	David Thorne	Pepco Holdings Inc & Affiliates	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mark Jones	Pepco	RFC	1

21.	Group	Rick Terrill	Luminant					X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mike Laney	Luminant Generation Company LLC	ERCOT	5
2.	Tim Soles	Occidental Power Services, Inc.	ERCOT	6
3.	Tim Soles	Occidental Power Services, Inc.	ERCOT	3
4.	Andy Gallo	Austin Energy	ERCOT	1
5.	Andy Gallo	Austin Energy	ERCOT	3
6.	Andy Gallo	Austin Energy	ERCOT	4
7.	Andy Gallo	Austin Energy	ERCOT	5
8.	Andy Gallo	Austin Energy	ERCOT	6
9.	Brenda Hampton	Luminant Energy Company LLC		

22.	Group	Joe Tarantino	SMUD & BANC	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Kevin Smith	BANC	WECC	1

23.	Group	Scott Brame	NCEMC	X				X					

	Additional Member	Additional Organization	Region	Segment Selection

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1. Robert Thompson		NCEMC	SERC 1										
24.	Group	Lesley Bingham	SPP and specific Member companies	X	X	X		X	X				
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Rayburn Country Electric Cooperative			SPP										
2. Empire District Electric			SPP	1									
3. City Utilities of Springfield			SPP	4									
4. Westar Energy			SPP	1, 3, 5, 6									
5. Cleco Power			SPP	1, 3, 5, 6									
25.	Group	Steve Rueckert	Western Electricity Coordinating Council										X
No additional members listed.													
26.	Group	Pawel Krupa	Seattle City Light	X		X	X						
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Pawel Krupa			WECC	1									
2. Dana Wheelock			WECC	3									
3. Hao Li			WECC	4									
27.	Group	Tom Flynn	Puget Sound Energy, Inc.	X		X		X					
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Denise Lietz		Puget Sound Energy	WECC	1									
2. Erin Apperson		Puget Sound Energy	WECC	3									
28.	Group	Michael Mertz	PNM Resources	X		X							
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. Laurie Williams		Public Service Co. of New Mexico	WECC	1									
2. Michael Mertz		Public Service Co. of New Mexico	WECC	3									
29.	Group	Sasa Maljukan	Hydro One	X									
Additional Member		**Additional Organization**	**Region**	**Segment Selection**									
1. David Kiguel		Hydro One	NPCC	1									
30.	Individual	Gerald Freese	AEP Standards based SME list	X		X		X					
31.	Individual	Benjamin Beberness	Snohomish County PUD										
32.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
33.	Individual	Antonio Grayson	Southern Company Services, Inc.	X		X		X	X				
34.	Individual	Brandy A. Dunn	Western Area Power Administration	X					X				
35.	Individual	Sara McCoy	Salt River Project	X		X		X	X				
36.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)			X	X						
37.	Individual	Nathan Smith	Southern California Edison Company	X		X		X					
38.	Individual	Jim Eckelkamp	Progress Energy	X		X		X	X				
39.	Individual	Tommy Drea	Dairyland Power Cooperative	X		X		X					
40.	Individual	John Brockhan	CenterPoint Energy	X									
41.	Individual	Tracy Sliman	Tri-State G&T - Transmission	X									
42.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				
43.	Individual	David Proebstel	Clallam County PUD No.1			X							
44.	Individual	John Falsey	Edison Mission Marketing & Trading					X					
45.	Individual	Brian Evans-Mongeon	Utility Services Inc.								X		
46.	Individual	Anthony Jablonski	ReliabilityFirst										X
47.	Individual	Jianmei Chai	Consumers Energy Company			X	X	X					
48.	Individual	Scott Bos	Muscatine Power and Water			X							
49.	Individual	Marcus Freeman	North Carolina Municipal Power Agency #1 and North Carolina Eastern Power Agency			X							
50.	Individual	Frank Dessuit	NIPSCO	X		X		X	X				
51.	Individual	Heather Laws	Portland General Electric	X		X		X	X				
52.	Individual	Michael Falvo	Independent Electricity System Operator		X								
53.	Individual	Cristina Papuc	TransAlta Centralia Generation LLC					X					
54.	Individual	Steven Powell	Trans Bay Cable	X							X		
55.	Individual	G. Copeland	Pattern					X					
56.	Individual	Chris de Graffenried	Consolidated Edison Co. of NY, Inc.	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
57.	Individual	Edward Bedder	Orange and Rockland Utlities Inc.	X		X							
58.	Individual	Michael Jones	National Grid	X									
59.	Individual	Mario Lajoie	Hydro-Quebec TransEnergie	X									
60.	Individual	Thomas A Foreman	Lower Colorado River Authority					X					
61.	Individual	Eric Scott	City of Palo Alto			X							
62.	Individual	Ed Nagy	LCEC	X		X							
63.	Individual	Robert Mathews	Pacific Gas and Electric Company	X		X		X					
64.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
65.	Individual	Michelle R D'Antuono	Ingleside Cogeneration LP					X					
66.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
67.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
68.	Individual	Michael Schiavone	Niagara Mohawk (dba National Grid)			X							
69.	Individual	Yuling Holden	PSEG	X		X		X					
70.	Individual	Jonathan Appelbaum	United Illuminating Company	X									
71.	Individual	John Souza	Turlock Irrigation District			X							
72.	Individual	Alice Ireland	Xcel Energy	X		X		X	X				
73.	Individual	Russ Schneider	Flathead Electric Co-op			X	X						
74.	Individual	Chris Higgins on behalf of BPA CIP Team	Bonneville Power Administration	X		X		X	X				
75.	Individual	Larry Watt	Lakeland Electric	X		X		X					
76.	Individual	David R. Rivera	New York Power Authority	X		X		X	X				
77.	Individual	Ron Donahey	Tampa Electric Company	X		X		X	X				
78.	Individual	Brian S. Millard	Tennessee Valley Authority	X		X		X	X				
79.	Individual	Thomas Washburn	FMPP						X				
80.	Individual	Annette Johnston	MidAmerican Energy Company	X		X		X	X				
81.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric					X					

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Company										
82.	Individual	Bob Thomas	Illinois Municipal Electric Agency				X						
83.	Individual	Richard Salgo	NV Energy	X		X		X					
84.	Individual	Steve Karolek	Wisconsin Electric Power Company			X	X	X					
85.	Individual	Ralph Meyer	The Empire District Electric Company	X									
86.	Individual	Daniel Duff	Liberty Electric Power LLC					X					
87.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
88.	Individual	Kirit Shah	Ameren	X		X		X	X				
89.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
90.	Individual	Brian J Murphy	NextEra Energy, Inc.	X		X		X	X				
91.	Individual	Christina Conway	Oncor Electric Delivery Company LLC	X									
92.	Individual	Gregory J. LeGrave	Wisconsin Public Service Corporation and Upper Pennisula Power Company			X	X	X					
93.	Individual	Don Jones	Texas Reliability Entity										X
94.	Individual	Don Schmit	Nebraska Public Power District	X		X		X					
95.	Individual	Stephanie Monzon	PJM Interconnection		X								
96.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
97.	Individual	Kathleen Goodman	ISO New England		X								
98.	Individual	Scott Harris	Kansas City Power & Light	X		X		X	X				
99.	Individual	Nick Lauriat	Network & Security Technologies, Inc.								X		
100.	Individual	John Allen	City Utilities of Springfield, MO				X						
101.	Individual	Scott Miller	MEAG Power	X		X		X					
102.	Individual	Nathan Mitchell	American Public Power Association			X							
103.	Individual	Jennifer White	Alliant Energy			X		X					
104.	Individual	Tracy Richardson	Springfield Utility Board			X							
105.	Individual	Maggy Powell	Exelon Corporation and its affiliates	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
106.	Individual	Scott Berry	Indiana Municipal Power Agency				X						
107.	Individual	Gregory Campoli	NYISO		X								
108.	Individual	Linda Jacobson-Quinn	Farmington Electric Utility System			X							
109.	Individual	Scott Kinney	Avista	X									
110.	Individual	James TUcker	Deseret Power	X									
111.	Individual	Warren Rust	Colorado Springs Utilities	X		X		X					
112.	Individual	Steve Alexanderson	Central Lincoln			X	X					X	
113.	Individual	Oscar Alvarez	Los Angeles Department of Water and Power	X		X		X					
114.	Individual	John Tolo	Tucson Electric Power	X									
115.	Individual	Russell A. Noble	Cowlitz County PUD			X	X	X					
116.	Individual	Tony Kroskey	Brazos Electric Power Cooperative	X									
117.	Individual	Darcy O'Connell	California ISO		X								
118.	Individual	Martin Bauer	US Bureau of Reclamation					X					

Questions with Summaries Included:

QUESTION D8 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified some of the definitions. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

BES Cyber Asset

Several commenters stated that the definition of BES Cyber Asset was confusing, citing the complex construction of the definition and the fact that it stated that each BES Cyber Asset must be part of a BES Cyber System while the background and technical basis stated that Responsible Entities had flexibility in using BES Cyber Asset or BES Cyber Systems. Many provided alternative language. Multiple commenters asked whether there is a need for network connectivity between BES Cyber Assets to be considered a BES Cyber System. The SDT made the addition of the statement about each being part of at least one BES Cyber System to the definition of BES Cyber Asset to ensure that each Cyber Asset would be included in at least one BES Cyber System, and did not preclude the option of having a BES Cyber System that consists of a single BES Cyber Asset. The SDT believes this preserves entities' flexibility while providing better homogeneity in the application of requirements: requirements uniformly apply to BES Cyber Systems. There is no presumption of connectivity options in the definition of a BES Cyber System, but Responsible Entities may find that application of requirements and relationship with other definitions such as ESPs may be significant input to the Responsible Entities' options.

Several commenters suggested that the definition of BES Cyber Asset include an addition in its qualification for connection to a network within an ESP in addition to connection to a Cyber Asset within an ESP. The SDT believes that the clarification is useful in ensuring the application to those transient cyber assets that are connected to the network as well as directly to the Cyber Assets within an ESP and has made the modification to address the comment.

One commenter suggested modifications to definitions of Cyber Asset. The SDT considered these comments and does not believe that these suggestions are substantively different or would add clarity to the definitions.

One commenter suggested dropping the word "misused" from the definition of BES Cyber Asset. The SDT has specifically included the word "misuse" in response to comments from FERC Order 706 and believes that it includes intent of a malicious compromise that is not otherwise conveyed.

Mid-American's comment with respect to the use of the capitalized term "Systems" has been addressed and the definition now used the more generic term "systems" instead of the defined term.

One comment was on the use of the verb phrase "affect the reliable operation…" The SDT considered these comments and believes that this verb phrase is appropriate as it applies to the Facilities, systems and equipment, not the BES Cyber System.

Many commented on the complexity of the parenthetical sentence in the definition of BES Cyber Asset and suggested alternative language: the SDT considered these comments and believes that the suggested alternatives do not add additional clarity to the definition. In addition, other commenters stated that the parenthetical qualification should be used in defining the term Transient Cyber Asset. The SDT considered the options and chose to not have a separately defined term because of the very small number of requirements where it is used.

Many entities commented on the use of "adversely impact" in the definition of BES Cyber Asset and suggested using the defined term "Adverse Reliability Impact" instead. The SDT considered the use of the defined term and believes that the defined term describes an impact which is much more severe than the intent of the term used in the definition.

Several commenters requested clarification of the terms "within 15 minutes": the SDT has included additional clarification in the guidelines and technical basis section.

–One commenter suggested to remove the 15 minute criteria as it is believed that it will lower the security of assets by removing them from qualifications. In response, The SDT notes that, in using 15 minutes, it is attempting to articulate a time boundary for "Real-time" impact. The term "Real-time" in the Glossary of Terms used in NERC Reliability Standards did not provide enough specificity in the definition for this purpose. The SDT scoped the CIP standards to those Cyber Assets that would have an effect on Real-time operations.

Many entities commented on the qualification on “redundancy” in the definition of BES Cyber Asset. The SDT believes that the impact of a cyber asset on the function of a given Facility, system or equipment is independent on whether that Facility, system or equipment is redundant or not: in most cases, the redundancy is configured to handle loss of a Facility, but does not consider degradation or misuse of that Facility, system or equipment. The application guidelines and technical basis section contains a discussion of this concept.

One entity suggests that the definition of BES Cyber Asset is much improved still does not prescribe how to document that an asset has been connected to the BES for less than 30 days. It is not the purpose of the definition to prescribe methods of documentation. That flexibility is left to the entity. Assets connected on a transient, temporary basis are not intended to be a BES Cyber Asset, and the 30 days in the definition is intended to clarify that temporary connections, e.g., for maintenance purposes, are not intended to be included within the definition.

BES Cyber Systems

One commenter suggested replacing “to perform” with “used to facilitate the performance of…”, citing examples where the BES Cyber System may not directly perform a reliability function, but may support one or more functions. The SDT believes that the introduction of the proposed language would result in further questions on the meaning of the word “facilitate” and the extent of the scope of that term.

In response to a suggestion to use the word “identified for functions…” the SDT believes that the suggested wording did not bring additional clarity to the definition of BES Cyber Systems.

One commenter stated that the use of the term “Responsible Entity” is confusing, citing overlap, redundancy or conflict with the term Functional Entity. The SDT believes that these are two distinctly different terms: the Responsible Entity refers to the set of Functional Entities that is responsible for compliance to the requirements of the standard. Within a given standard, a given set of requirements may apply to different Functional Entities, depending on the specific requirements. The term “responsible entity” is defined in the applicability section. The application of the defined term that contains the term “responsible entity” in a standard is subject to the preamble in Section 4.

Cyber Asset

Multiple comments were provided on the use of the word “programmable” in the definition of Cyber Asset, citing that it was too broad, and the need for a routable connectivity qualification. The SDT considered these comments and notes

that the definition of Cyber Asset as it pertains to “programmable electronic devices” is part of the current approved definition. The SDT further believes that consideration of connectivity in this generic definition is inappropriate.

One commenter stated that the qualification of “…data in these devices…” ignores data in motion. The SDT believes that the inclusion of data other than that in these devices has unintended consequences in the application of requirements.

Other

Multiple commenters suggested the addition of a defined term BES Site, or similar concepts: the SDT has considered the rationale and has opted to use the concepts in the drafting of new language and approach in the requirement language and attachments, instead of defining a term that would be used in only a few requirements.

One commenter requested that the language for the defined term Protected Cyber Asset be reviewed for clarity. The SDT has reviewed the definition and made modifications to the definition and added guidance in the background section to clarify the concept.

QUESTION D9 – DEFINITIONS:

Do you have any comments on the changes to the proposed definition of Control Center? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:

Based on stakeholder comments, the SDT modified all of the definitions based on stakeholder comments. The explanations below describe the significant modifications made based on stakeholder comments – the SDT made other minor edits for improved clarity. Please see the redlined version of the definitions for a complete set of revisions to each definition.

Many commenters questioned the need for a definition of Control Center, citing standards in other reliability standards that also have control center applicability without the need for a formal definition. The SDT notes that the Control Center is subject to a number of High and Medium Impact criteria and that they host a large number of BES Cyber Systems that are essential to the reliable operation of the BES. The SDT believes that, because of these necessarily crucial functions, a formal definition is appropriate to clearly define the scope of applicability, as demonstrated by many questions on differentiation between a facility's control room, which is typically considered part of the facility, and Control Centers, which are considered separate facilities hosting operating personnel controlling and monitoring multiple facilities. Many commented that a formal definition used in the CIP context could be confusing to the industry in the context of other reliability standards that apply to control centers. The SDT believes that a formal definition clarifies the scope of applicability for Control Centers and would not affect other reliability standards that have not used the defined term, but rather a "common" undefined term for control center. NERC's standard use of capitalized terms for NERC Glossary defined terms provides clarity on when the defined term is used.

Two commenters proposed alternative language for the definition of the Control Center that uses Functional Entities. The SDT has considered the alternatives and believes that the proposals contain a circular reference that would not provide better clarity. The SDT has carefully considered the current proposed language and believes that it accurately describes the intended target of applicability.

Others suggested that Control Centers that use voice or manual instructions be categorized as Low Impact. The SDT notes that Cyber Systems that provide information to Control Center operators that use manual or voice to effect control operations on BES assets in real-time based on that information must be subject to the same protection as those that

trigger automated operation. If the communication or manual operation results from information provided for real-time operations, there is no rationale for categorizing them as a lower impact.

Multiple commenters expressed concern that in certain instances, a facility may not be performing the function of a TOP 24/7 and remains unmanned the rest of the time, and suggested the addition of the 24/7 qualification. The SDT sees no rationale in adding this qualifier, since the impact of the facility that performs these functions remains the same. In the same comment, commenters cited the case of a TOP registration for a single facility. The SDT responds that the "control and monitoring" facility of a single facility does not meet the definition of a Control Center, but rather as part of the facility it is controlling.

Several commenters suggested slightly modified language which focuses on hosted BES Cyber Systems rather than operating personnel. One commenter suggested that the Control Center is the BES Cyber System that performs these functions. The SDT believes that operating personnel is central to the traditional understanding of a Control Center facility. The definition currently specifies one or several facilities. In the facilities (or site) based approach, the identification of the BES Cyber Systems that perform the Control Center functions may bring in other facilities such as data centers that perform these functions.

Many commenters requested clarifications on the terms "facility" and "locations" used in the definition of the Control Center. The SDT uses the general term "facility" (as opposed to the glossary term "Facility") in its generic sense of one or several physical structures that comprise a Transmission substation or station, a generating plant or a Control Center. In the case of a Control Center, a facility could be considered a building or campus consisting of several closely located buildings. However, additional facilities may be brought in as the BES Cyber Systems are defined, including associated data centers that perform the reliability tasks. In the context of the definition of Control Center, a location generally refers to the set of BES Facilities at a single site, and generally constitutes a single point of connection to the BES. Because of the many types of configurations, the SDT used the generally accepted concept of geographic location rather than including all the nuances of the different ways Facilities are connected to the BES.

One commenter requested a definition for data center. The SDT believes that "data center" is a well understood term and that many definitions of data center exist elsewhere that adequately explain what they are.

One commenter pointed out that the SDT uses the term reliability functional tasks and reliability tasks interchangeably in the standard. The SDT has used the terms interchangeably for the reliability tasks defined in the NERC functional model. The SDT has made the change in the definition of Control Center to be consistent to the use of reliability tasks elsewhere.

One commenter requested further qualification of the term “operating personnel”. The SDT notes that this term is used in many reliability standards, in particular, the PER series of standards. They are used to refer to personnel that perform the real-time control and monitoring operations necessary for the real-time functions for RC, BA, TOP and GOP functional entities. The definition of the Control Center refers to these functions.

One commenter suggested the addition of “NERC Certified” to operating personnel. The SDT notes that the addition of the term NERC Certified restricts the applicability of the term to just RCs, BAs and TOPs, since there is no requirement for certification of GOP operating personnel. This is not the intent of the SDT in drafting this definition.

One commenter suggested that Control Center as it applies to the function of a Generation Operator has a threshold of generation located at two or more locations, and that this single qualifier could unintentionally sweep in the control centers for multi-location generation of very small capacity. The commenter suggested that a capacity qualifier be added to this definition. The SDT does not think that the threshold should be in the definition, but has amended the criterion for generation Control Centers in the Medium Impact category that addresses this comment. BES Cyber Systems for Control Centers below the Medium Impact threshold must still be protected as Low Impact. See the response to A03 - Attachment 1, Medium Impact.

QUESTION D10 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the comments related to these definitions largely noted minor improvements to the definitions rather than identifying major issues or disagreement.

BES Cyber System Information
Several comments about the definition of BES Cyber System Information highlighted minor issues with the structure of the definition rather than its content. Commenters suggested re-organizing the definition such that the list of examples came last. The SDT considered this comment and agreed that it made the definition more readable without changing its overall intent. This suggestion has the effect of collecting the explanatory language together to improve comprehension of the definition. Some commenters suggested that the examples should be removed from the definition altogether. The SDT noted that it is not uncommon to find examples in definitions in the NERC Glossary of Terms Used in NERC Reliability Standards (e.g. Facility, Operating Plan, Year One, etc.). Additionally, the SDT had concerns about removing the list of examples, since a similar list of examples has been used since the version 1 CIP Standard to provide direction as to what information should be included in the NERC CIP information protection program. The SDT believed that continuing to provide a list of examples would facilitate a transition between Version 3 and 4 of the CIP standards to Version 5.

Additionally, some commenters took issue with the phrase "developed by the Responsible Entity" as it relates to security procedures and security information. The commenters noted that protection of security information might be appropriate even if this information was developed by an outside party. The SDT agrees with this comment. The intent of the SDT was to prevent the inclusion of information that might be publicly available. Therefore, the SDT has modified the definition to better align with the intent and has clarified that security procedures and security information "not publicly available" are examples of BES Cyber System Information.

Some commenters noted ambiguity in the definition of BES Cyber System Information in the phrase "unauthorized distribution" of information. The SDT appreciates the concern over ambiguity, but encourages the industry to consider this definition in context of the overall information security program that is required under NERC CIP-011-1 and related

requirements in NERC CIP-004-5. Consideration of "unauthorized distribution" should be taken in the context that access to locations where information that has been judged to meet this definition is stored is required to be authorized in CIP-004-5 R4, part 4.1, element 4.1.3 and proper handling of this information is required in CIP-011-1 R1, part 1.2. The Responsible Entity should use this context to determine whether this information, in the hands of someone who has not been granted access "based on need," could lead to a compromise in security, directly or indirectly, of the BES Cyber System.

Other commenters noted ambiguity over the phrase "pose a security threat" and recommended that this phrase be removed. The concept of posing a "security threat" to the BES Cyber System should also be considered in context of the requirements of the NERC CIP Standards, particularly CIP-011-1 R1. BES Cyber System Information is intended to be identified and protected in accordance with an overall information protection program. As such, it is anticipated that the Responsible Entity will include some process to identify the information applicable to this program. As not all information will lead to directly gaining access to BES Cyber Systems but may in other ways compromise the overall security of the BES Cyber System, the SDT does feel that it is prudent to remove this phrase.

CIP Exceptional Circumstances

Several commenters identified an issue with the phrase in the definition of CIP Exceptional Circumstances that included "an imminent or existing hardware, software, or equipment failure." Commenters pointed out that the collection of forensic data in CIP-009-5 Requirement R1.5, draft 2 was subject to CIP Exceptional Circumstances. Through the inclusion of hardware, software, or equipment failure as a CIP Exceptional Circumstance, a Responsible Entity could essentially choose to never comply with the collection of forensic data. After consideration, the SDT chose to modify the requirement in CIP-009-5 R1.5 to indicate that data preservation should not impede or restrict recovery. The SDT believes that hardware, software, or equipment failure is a reasonable component to include as a CIP Exceptional Circumstance given the cyber-physical relationship of the electric grid and its supporting Cyber Assets.

Additionally, commenters noted that the involvement of the conditions identified in the definition of CIP Exceptional Circumstances is not always known ahead of time. Specifically, commenters suggested that the SDT add the phrase "threatens to involve." The SDT considered this suggestion and decided that given the supporting framework required through the cyber security policies in CIP-003-5 to invoke a CIP Exceptional Circumstance, this was a reasonable and beneficial modification to the definition.

Commenters also questioned when CIP Exceptional Circumstances can be invoked. No modification was made to the standard, but in response, the intent of the SDT is to allow the use of CIP Exceptional Circumstances only where specifically identified in the language of the requirement. Additionally, CIP Exceptional Circumstances should be declared using the provisions identified in the Responsible Entity's cyber security policy as per CIP-003-5 R1.

CIP Senior Manager

Numerous commenters suggested minor modifications to the definition of CIP Senior Manager. The intent of the SDT was to include a definition of CIP Senior Manager in the NERC Glossary of Terms Used in NERC Reliability Standards so as to make clear who the required approver is when the term is used across the body of CIP Standards. The SDT did not intend to modify the content of the definition, which has remained unchanged since version 2 of CIP-003-2 when the role of the senior manager was clarified in response to FERC Order 706, paragraph 381. The SDT was compelled, given the current state of the CIP Standards being in their 5th version, by comments that suggested that in addition to the authority and responsibility for leading and managing the implementation of the requirements, that the CIP Senior Manager should also have the overall authority and responsibility for leading and managing "continuing adherence" to the requirements within the NERC CIP standards.

The SDT also received comments that the definition of CIP Senior Manager should specifically call out CIP-002 through CIP-011 as this is the set of cyber security standards to which the CIP Senior Manager has the authority and responsibility for. The SDT received similar comments in response to draft 1 of the posting of this definition. At that time, the SDT responded that the definition was only applicable where it is specifically used in the standards. Additionally, the concern appeared to specifically reference CIP-001, which at the time was planned for retirement as part of project 2009-1. However, given the dynamic nature of project 2009-1 and the relative ease to which this definition could be modified in the future should additional standards be added to which the CIP Senior Manager authority should apply, the SDT is persuaded to include a reference specifically to "CIP-002 through CIP-011" in the definition of CIP Senior Manager.

QUESTION D11 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Physical Access Control Systems and Physical Security Perimeter? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the SDT has address all comments and has made clarifying changes to the definitions.

Physical Security Perimeter (PSP)
One commenter proposed modifying the definition to apply only for applicable BES Cyber Systems. However, applicability cannot be determined by a definition. We have clarified in the applicability column in standards CIP-004 through CIP-011 that PSPs are not applicable solely upon meeting the definition.

One commenter requested that a list of example Cyber Assets that should be included within a PSP. In response, the standards specify more clearly which Cyber Assets must reside in a PSP.

One commenter suggested the definition of PSP should reference the correct defined term: Electronic Access Control or Monitoring Systems, and the SDT has made this change.

One commenter suggested that the definition is ambiguous about (1) whether the perimeter is two or three dimensional, (2) whether there are different expectations for High and Medium BES Cyber Systems and (3) what size hole provides access. In response, the additional specificity for the perimeter and access points would limit the options entities have in applying the requirement. The SDT believes we have struck the right balance in this requirement to allow entities flexibility in their approach while describing the end result. In regard to the difference between physical protection in High and Medium Impact BES Cyber Systems, this is specified in CIP-006-5.

Physical Access Control System (PACS)
Several commenters proposed removing "alert" from the definition to avoid the interpretation that security guard workstations are included in scope. In response, the alerting component should include the system sending out the alert

and does not include all recipient persons or devices of the alert. We do not believe this needs further clarification in the definition.

One commenter suggested that examples should not be included in the definition and the wording “exclusive of devices…at the PSP” could exclude more asset than intended. In response, we note that examples should not change the definition but can be helpful in forming context. For PACS, these examples are useful for explicitly clarifying perimeter devices, which by nature cannot have the same physical protection are outside of scope.

One commenter suggested putting a comma to make clear the example applies to Cyber Assets. In response, the example does modify the locally mounted hardware and devices and not the Cyber Assets. In other words, the example is for the exclusion.

One commenter suggested that the SDT needs to ensure electronic visitor log books are not captured in the definition and that the exclusion uses “or” instead of “and” for the examples. In response, a visitor log book would not be within scope because it logs visitors and not access, and including an electronic visitor log book could cause the interpretation that any additional logging would be considered out of scope. Also, “or” and “and” are logically interchangeable in the example list, and we do not find a need to make any change.

One commenter suggested that monitoring Cyber Assets should be included in the definition. In response, we did not include monitoring devices because those are typically outside of the PSP and serve as a supplementary protection. Although these can be used to comply with monitoring requirements, it becomes problematic to apply additional CIP Standards requirements without creating a complex protection loop.

One commenter suggested changing the word “exclusive” to “excluding”, but the SDT chooses to retain the originally posted wording.

One commenter suggested the definition should include workstations used to provision physical access and monitor alarms. In response, the proposal would expand the definition scope beyond what the SDT considers unacceptable risk. The level of effort required to protect this significant population of assets would far exceed the security benefit of doing so. As an example, this could include all cell phones and pagers carried by staff for responding to alarms.

QUESTION D12 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Control and Monitoring Systems, Interactive Remote Access, and Intermediate Device? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, clarifying language was added to each definition to highlight stakeholders concerns.

Interactive Remote Access
Several commenters requested clarification for the inclusion of dial-up access in the definition. Upon further review, this has been removed from the definition. The important part to note is that Interactive Remote Access is when using a remote access client or other remote access technology, regardless of the type of connectivity.

One commenter proposed that the definition of Interactive Remote Access be modified to exclude serially connected, non-routable, non-network connected devices. The definition did not include serially connected, non-routable, non-network connected devices. However, the definition has been modified to specifically address the use of a routable protocol.

Several commenters requested restructuring of the definition to highlight the criteria for identifying Interactive Remote Access. The definition has been updated as requested to highlight that the first criteria is the use of a remote access client or other remote access technology.

Several commenters requested more information regarding examples of a remote access client or remote access technology. Additional information is available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that list item two, "Cyber Assets used or owned by employees" be modified as "Cyber Assets used by employees". The commenter considers employee-owned devices inappropriate for use in Interactive Remote Access. Employee-owned devices were added to the definition based on comments received in Project 2010-15:

Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

One commenter recommended adding the words “owned by or under the control of the Responsible Entity” to prevent the inclusion of equipment owned by Managed Security Providers in the standards. Connections by vendors, contractors, and consultants should be protected to the same standard as assets owned by the entity. Assets owned or used by vendors, contractors, and consultants were added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. This is in support of pandemic and other emergency planning situations.

Multiple commenters noted that the sentence beginning with “Remote access may be initiated from ...” adds no value, does not address all circumstances, and should be deleted. They further noted it is possible to initiate remote access from assets owned by others not listed. The information was added to the definition based on comments received in Project 2010-15: Expedited Revisions to CIP-005-3. This was added to address industry need to have remote access not limited to use of only company-owned assets for remote access. Please see the opposing perspective noted by other entities. The definition states that access “may be initiated” and not “shall be initiated” to allow for flexibility and not define the three scenarios as the finite and final list.

Intermediate Device

One commenter was concerned with the phrase “performing access control” existing as part of the definition of an Intermediate Device. It is the SDTs intent that an Intermediate Device is classified as an Electronic Access Control or Monitoring System. The definition of Electronic Access Controls or Monitoring Systems has been modified to include Intermediate Device.

One commenter requested clarification as to the types of devices that could be used as an Intermediate Device. The SDT specifically did not list proxy or other technology to allow flexibility in how an entity may implement a solution that best meets their needs. Per CIP-005-5 Requirement R2.1, the Intermediate Device must be used before accessing a BES Cyber System or Protected Cyber Asset. Per the definition, the Intermediate Device must not be inside of an ESP. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Multiple commenters noted concerns with the language, “The Intermediate Device must not be located inside the Electronic Security Perimeter”. Comments were received that this should be added to the requirements and removed from the definition. Some consider the second sentence of the definition to be unnecessary, too prescriptive, and should be deleted. Some offered recommendations for changes to the definition to allow for future technology developments.

- The SDT considers this language to be defining and clarification of the device. The performance under the requirement is that an entity utilizes the intermediate device. Further, definitions are part of the standards and carry the same force as the requirements.
- The location of the Intermediate Device was included in the definition to address numerous industry questions on this matter both in Project 2008-06 Cyber Security Order 706 Version 5 CIP standards and Project 2010-15: Expedited Revisions to CIP-005-3. Many entities have raised questions regarding the location of the device based on termination point of encryption and other issues.
- The only restriction placed on the Intermediate Device is that it not be inside of an ESP. Access authentication should be performed before the user is granted access through the ESP. Encryption should be terminated outside of the Electronic Security Perimeter so that event logging within the ESP is not negatively impacted. The SDT specifically did not list other specifics to allow flexibility in how an entity may implement a solution that best meets their needs whether through the use of a multi-purpose device or other architecture. Additional references regarding the Intermediate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter noted concerns that the term "device" is not clear in defining the Intermediate Device. They recommend using the term “Intermediate Cyber Asset”. The definition includes the term “Cyber Asset” which is defined as “programmable electronic devices including the hardware, software, and data in those devices”. The SDT has chosen the unique term “Intermediate Device” to allow for the use of one or more Cyber Assets making up the device.

QUESTION D13 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, the SDT clarified language to the definitions.

Electronic Access Point
Multiple commenters asked for clarity if an Electronic Access Point (EAP) must be routable on both sides. In response, the SDT's intent is that if the device is accessible from outside the Electronic Security Perimeter (ESP) with a routable protocol then an EAP must be put in place. Therefore, just as in the Critical Cyber Asset Identification Guidelines of today, the 'inside' does not have to be routable. For example, if the entity has a digital relay and has the serial port used for console access (non-routable serial communications) attached to a serial-to-IP gateway such that the relay's command console is addressable from outside the ESP via a routable protocol (e.g. <IP Address>:<Port #> will connect you to the relay), then this meets the definition of External Routable Connectivity and an EAP is required.

One commenter provided an alternate definition that included the phrase "externally routable bi-directional communication" and added "or inbound communications to a Cyber Asset within the Electronic Security Perimeter" to the end. In response, the SDT notes that the direction of the communication is an aspect of External Routable Connectivity definition. The Electronic Access Point is an intentionally broader definition and its main function is to deny all access by default and only allow needed traffic to cross the ESP, regardless of direction.

One commenter asked that it be clarified as to whether an EAP is part of the ESP or not? In response, the SDT notes that an EAP is part of an ESP as it is the point where the routable communication from outside the ESP is allowed to cross the ESP to Cyber Assets inside the ESP.

One commenter suggested that the term "interface" be removed and have the definition reference a Cyber Asset. In response, the SDT notes that the inclusion of interface is meant to address the situation where an entity has a firewall as an EAP that has numerous interfaces to different networks and only one goes to a network that has applicable Cyber

Assets. The inclusion of 'interface' means the requirements would be concerned with only those interfaces that communicate with applicable Cyber Assets and not to interfaces that do not have any applicable Cyber Assets. The SDT also notes that the requirements in CIP-005 that apply directly to EAPs concern an interface (deny by default, methods for inspecting for malicious communications, etc).

One commenter suggested that the definition add "allows or is capable of allowing" to include dual homed Cyber Assets including laptops with wifi that is not hardware disabled. In response, the SDT believes that for a mandatory requirement the enforceable point should be binary – either communication is allowed to cross an ESP or it isn't – and the standards should avoid dealing with all possible capabilities.

One commenter asked for confirmation of the notion that Cyber Assets only communicate with other Cyber Assets. In response, the SDT notes that Cyber Asset is the basic unit of these standards and there is no lower level term. As Cyber Asset is a 'programmable electronic device', the SDT believes this covers most all situations. The SDT notes that Cyber Assets includes most all network gear as well, not just servers and workstations.

Electronic Security Perimeter

Several commenters suggested that examples should be included. In response, the SDT is not including examples in this term. Since terms such as ESP often refer to cyber technology that is constantly changing and developing, there is a tendency for examples to become outdated. The SDT used guidance instead to discuss examples rather than definitions. When the term is then used in a requirement, there is a tendency for the examples to then become prescriptive and mandatory, which is not the purpose of examples.

Multiple commenters provided some clarifying questions: Does an ESP presume the presence of EAP? Does a BES Cyber System with no External Routable Connectivity fall into scope? In response, the SDT clarifies that the ESP does not presume the presence of an EAP and BES Cyber Systems without External Routable Connectivity are in scope of the CIP standards. The ESP is a 'logical border' around a routable protocol network to which a BES Cyber System is connected. An isolated network with no external connectivity has an ESP; a logical border. The ESP is used to determine the 'Associated Protected Cyber Assets' as well as the collection of Cyber Systems and Assets that will be elevated to the impact level of the highest impact BES Cyber System/Asset in the ESP (see the definition of Protected Cyber Asset). If routable protocol communications cross the ESP, then an EAP is required.

Several commenters stated that this should be applicable to BES Cyber Asset instead of BES Cyber System. In response, the SDT notes that the BES Cyber System grouping is up to the entity and the concepts of electronic and physical security perimeters need to be taken into account. An entity is free to define every individual BES Cyber Asset as its own unique BES Cyber System and in essence make the entire standard Cyber Asset based. The grouping into systems is at the entity's discretion, but should be done with the requirements in mind.

External Routable Connectivity

Multiple commenters suggested that clarity is needed concerning the focus on Cyber Asset connectivity, rather than a 'system' with connectivity. Does a 'system' with one routable device mean all cyber assets in the system meet the applicability? This applies to the ESP definition as well. In response, the SDT has updated the definition to be at the Cyber Asset level rather than the BES Cyber System level. The intent is that Cyber Assets that have External Routable Connectivity must meet the applicable requirements and Cyber Assets that do not meet the definition are exempt from the requirement.

Several commenters suggested that the definition should include the OSI network layers. The SDT has chosen to not include Open System Interconnection (OSI) layers in the definition at this point. It is believed that with the history of the CIP standards being based on 'routable protocol' since its inception that there is a sufficient understanding of these terms at this point.

Multiple commenters suggested that the definition should be reworded to be a property of a BES Cyber Asset, not the asset itself. In response, the SDT agrees and has changed the definition to begin with "The ability to access…"

One commenter suggested that the definition should only apply if routable connection goes all the way to a BES Cyber Asset within the ESP. In response, the SDT is trying to incorporate the situation (identified in the current CCA Identification Guidelines) where an Ethernet/serial gateway is used at the perimeter. A BES Cyber Asset may have a serial connection from its console port to the Ethernet/serial gateway such that from outside the ESP the device's console port is directly addressable using a routable protocol, usually simply in the form of <ip address:port #>. The SDT's intent is for the definition to capture any device that is accessible from outside the ESP with a bi-directional routable protocol.

One commenter suggested that the definition needs to consider inside to outside connectivity not just outside in. In response, the SDT does consider 'inside out' connectivity in the requirements (e.g. outbound rules on EAP's). However, the intent with this definition is to focus on the higher level of threat that outside-in connectivity presents as well as to

give some credit for more secure network architectures that only push data out and don't allow outside-in connectivity (data diodes, etc.).

A few commenters commented that the definition should be Cyber Asset based rather than strictly limited to BES Cyber Systems. In response, the SDT has clarified that access is from a Cyber Asset that is outside of the BES Cyber System's associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Protected Cyber Asset

Multiple commenters suggested that the parentheses should be removed, keeping the sentence concerning temporarily connected Cyber Assets. In response, the SDT agrees and has made the suggested change.

One commenter suggested that the temporarily connected Cyber Asset exclusion should be pulled out and made into a separate definition. In response, the SDT in this instance would be defining a term simply to use the term in the definition of another term. Therefore the SDT believes it is more straightforward to include a more complete definition in the ultimate term we are defining, and see no issue with stating what something is and what it is not while defining it.

Multiple commenters suggested that this should allow for network connection of temporarily connected Cyber Assets, suggesting that 'directly' be removed to allow connection within the ESP without requiring connection through a Cyber Asset. In response, the SDT notes that a network switch is a Cyber Asset and thus network connections are included. However, the SDT agrees that this point needs more clarity and has deleted the word 'directly' and clarified that it is a connection either to a Cyber Asset in the ESP or the network within an ESP.

One commenter suggested that a separate definition for Transient Cyber Asset should be included and have a requirement to scan for malware before connection. In response, the SDT notes that this was included in previous drafts but was removed in this draft in response to comments. Numerous comments were received pointing out the audit issues of such a requirement. How does one prove that a list of temporarily connected devices is complete? How does one prove that virus scans were done on a device that was there one minute and gone the next? How does one maintain and prove a complete inventory of all temporarily connected devices? Commenters also pointed out that the object of protection is the BES Cyber System – the goal is to protect BES Cyber Systems from all threats including temporarily connected devices. There were also numerous issues raised concerning TFE's as many troubleshooting and maintenance devices are 'programmable electronic devices' and would thus be Cyber Assets but have no antivirus available. A cable scanner used to diagnose cabling issues may be a programmable electronic device and then require a TFE. In response to

all these issues, the SDT decided to remove the requirement. However, the SDT notes that CIP-007 R3 requires an entity to deploy method(s) to deter, detect, or prevent malicious code and it is expected that such measures as scanning temporarily connected laptops and other similar devices may be included in these methods.

QUESTION D14 – DEFINITIONS:

Do you have any comments on the changes to the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident? If you voted "negative" on any ballot because of a proposed definition or modification to a definition described in this question, please describe the specific suggested changes that would facilitate an "affirmative" vote.

SUMMARY:
Based on stakeholder comments, several changes have been made to clarify language in the definitions.

General Comments
Several commenters stated that the phrase "reliability tasks of the functional entity" is unclear and needs to be replaced or further defined. In response, the phrase reliability tasks of the functional entity comes from the definition of BES Cyber System and the reliability tasks are those specified in the NERC Functional Model.

Several commenters suggested that the terms compromise and disrupt need to have their own definition. In response, the words compromise and disrupt carry forward from the previously approved definition and we have not received compelling indication that these terms need further clarification.

Several commenters suggested that the phrase "was an attempt to compromise" is vague and should be deleted. In response, this phrase captures those incidents that do not necessarily succeed but should prompt investigation.

One commenter suggested replacing the phrase "reliability tasks of the functional entity" with "reliability tasks identified for functions in the NERC Functional Model." The SDT does not specify the NERC Functional Model, which is not a document subject to the standards development process, but the SDT believes that the phrase adequately conveys those tasks.

One comment was on the phrase "malicious and suspicious" is subject to interpretation and proposed adding the qualifying phrase, "as determined by the Responsible Entity." In response, the definition should not include this phrase because it is not a requirement, and CIP-008-5 already specifies the obligation for the Responsible Entity to make this determination.

One commenter suggested qualifying the term ESP and PSP with BES Cyber System to avoid having to demonstrate compliance with perimeters that do not protect BES Cyber Systems. In response, the requirement in CIP-008-5 makes this distinction in the applicability section.

One commenter suggested that the definition of Control Center uses a different term "reliability functional tasks" and requests clarification if this term means something different. In response, the SDT has clarified the language to read "reliability tasks".

One commenter suggested that the DOE OE-417 form should be considered to allow entities to comply with both requirements. In response, the SDT has reviewed the latest version of this form and do not find any reporting requirements that would conflict with those in CIP-008-5.

Cyber Security Incident

Several commenters suggested replacing the phrase "was an attempt" with "has the potential" in the definition of Cyber Security Incident because an attempt implies knowing the intent of the perpetrator and it excludes accidents which have the potential to compromise the BES Cyber System. In response, we have not significantly changed the currently approved definition and do not find the need to incorporate the proposed modifications. Both phrases communicate the desired result that an unsuccessful attack or compromise would be considered a Cyber Security Incident.

There was a suggestion that the definition of Cyber Security Incident now includes PSPs and the impact will be difficult to assess. In response, the current approved definition includes PSPs.

One commenter proposed to amend the definition of Cyber Security Incident to include: "Is a violation or imminent threat of a violation of computer security policies, acceptable use policies, or standard security practices impacting or within covered ESPs or PSPs." In response, violation of policies can be covered in an entity definition of a cyber security incident, but the Glossary definition has a focus on impact in order to broadly apply the standard.

One commenter suggested that physical security incidents should have its own definition and not be included as part of a Cyber Security Incident. In response, a physical security breach into a perimeter protecting the BES Cyber System provides enough cause for concern in the integrity of the BES Cyber System to warrant classification of a Cyber Security Incident. Individual entities may use distinct terms and response teams for these types of incidents, and the obligations in CIP-008-5 would still apply.

Several commenters proposed removing the phrase “suspicious event” from Cyber Security Incident. In response, the term suspicious event captures those incidents prompting further investigation in which the entity may not determine the cause or motive.

Reportable Cyber Security Incident

SPP RE expressed concerns that Reportable Cyber Security Incidents would not include those incidents in which redundancy mitigated the impact. In response, we have provided guidance in CIP-008-5 that Reportable Cyber Security Incidents would also include those that triggered an activation of redundant systems.

There was a proposal to replace “Any” with “A” to start the definition of Reportable Cyber Security Incident and we have done so.

One commenter proposed the following definition of Reportable Cyber Security Incident: “Any Cyber Security event that has compromised or disrupted one or more reliability tasks of a functional entity, which through investigation and escalation, has been determined by the Responsible Entity to be reportable to ES-ISAC.” In response, this proposed definition includes a requirement, which should remain in the standard. The requirement in CIP-008-5 still provides leeway to the entity in determining Reportable Cyber Security Incidents.

One commenter stated that the definition needs to be coordinated with the EOP-004-2 drafting team. In response, both the CIP Version 5 and EOP-004-2 drafting teams have agreed to move all reporting obligations for Cyber Security Incidents to CIP-008-5.

One commenter proposed the definition for Reportable Cyber Security Incident in order to avoid using the term functional tasks, “A Cyber Security Incident that compromised the ESP or PSP or disrupted the operation of an applicable BES Cyber Asset or low BES Site.”

One commenter proposed to add additional guidance in CIP-008-5. In response, the use of functional tasks ties the reportable incident to a specific reliability function. Without this qualification, the definition can easily be interpreted to include nominal security events as reportable. The SDT has already added additional guidance on distinguishing a Reportable Cyber Security Incident.

QUESTION D16 – IMPLEMENTATION PLAN:

If you disagree with the changes made to the Implementation Plan since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, there were not many changes made to the Implementation Plan, but the comments and comment responses below provide clarity into some of the concerns regarding the proposed effective date, the possibility of bypassing Version 4, and the initial performance of certain periodic requirements.

Proposed Effective Date

One commenter suggested that the effective date conflicts with the initial performance of requirements section and should specifically mention this in the effective date language as an exception. In response, we do not feel this is necessary. The implementation plan enumerates any exceptions to the effective date of the standard. The alternative of including all such exceptions in the effective date language would make the language unreasonably complex.

One commenter agreed with the approach to focus on the high and medium impact BES Cyber Systems but questions the need for an additional year of implementation time for low impact BES Cyber Systems particularly if no inventory is necessary. SPP RE also agrees an additional year for compliance with CIP-003-5 R2 is unnecessary. In response, the need for an additional year of implementation for low impact BES Cyber Systems exists to allow entities to formulate and implement effective security solutions for physical and electronic perimeter protection. Despite not requiring an inventory of low impact BES Cyber Systems, entities must still implement these policy changes in applicable locations where no perimeter protection currently exists.

Several commenters questioned why the effective date is so far out given that the standards have been in development for more than two years. In response, the development timeframe of the standards do not determine when entities begin planning compliance. Rather, entities have assurance in the finality of the standards upon FERC approval. The number of cyber systems applicable in this standard far exceeds any previous version of the standard. The SDT reasons it will take two budget cycles for entities to plan and implement these standards.

Bypassing Version 4

Several commented that language to extend the Version 3 effective period and bypass Version 4 should be removed because the recent FERC Order has solidified the effective date for Version 4 as April 1, 2014. Other comments request a

transitional plan to address the period of compliance between Version 4 and 5. In response, the SDT observes that the provisions to bypass Version 4 remain in the implementation plan and are subject to approval by the industry and FERC. This is explained in greater detail in the summary section at the beginning of this document.

Initial Performance of Certain Periodic Requirements

One commenter stated that for non-periodic requirements, the IP should state entities comply with all other requirements on the effective date. In response, this is already stated in the effective date language. The periodic requirements are exceptions to this language.

Several commented that CIP-010-1 requirement part 3.2 and CIP-009-5 requirement part 2.3 have a 36 month periodic performance requirement and should have an initial performance not exceeding 36 months after the effective date. Yet, although the periodicity for this requirement is 36 months, the initial performance should occur closer to the effective date of the standard. However, we are persuaded by arguments that initial exercises should be conducted prior to the operational exercise active vulnerability assessment.

Several commented that the language "…Notwithstanding any order to the contrary…" is unnecessary because the FERC can approve or remand any part of the implementation plan if it so chooses. While this is true, the inclusion of this language allows that decision to be made without the tremendous overhead of going through the standards development process.

One commenter argued that the periodic requirements section requires compliance as early as 14 days after the effective date, but the effective date allows 24 months. In response, this is true, and all of the specified periodic performance requirements occur after the effective date, which is at least 24 months.

One commenter argued the initial performance of the requirement should be performed prior to the effective date. They questioned why a year would be necessary to hold the first training or verify provisioned access. In response, the SDT disagrees with compliance prior to the effective date for two reasons. First, the effective date of the standard indicates when Version 5 becomes effective and previous versions retire. Requirements that obligate performance on a specific day cannot technically be compliant prior to the effective date. Second, the specified periodic requirements are mostly verification assessments or updates for existing security controls, and the objective is to have the security controls in place upon the effective date.

Based on comments received, CIP-009-5 requirement part 2.3 has been added to the list of periodic requirements that must be implemented no later than 12 months after the effective date.

One commenter noted that CIP-009-5 Requirement R1.4 still contains language requiring an initial performance. However, the intent of this requirement was not to obligate an initial periodic performance, and we have modified the requirement language to remove the word "initial".

Planned or Unplanned Changes

Several commenters suggested all new or reclassified Cyber Systems have the same timeframe of 12 months to achieve compliance. In response, we have updated the implementation plan based on changes to CIP-002-5 that remove obligations to update the BES Cyber System categorization within 60 days. This provides entities additional time to demonstrate full compliance for planned changes. Unplanned changes resulting in a higher categorization continue to allow the additional year to demonstrate full compliance for the affected BES Cyber Systems.

The Planned or Unplanned Changes section was collapsed into one section based on multiple comments, and it has been clarified that for *planned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards on the update of the identification and categorization of the affected BES Cyber System, with additional time to comply for requirements as specified and in the same manner as in the section *Initial Performance of Certain Periodic Requirements*. For *unplanned* changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in the Version 5 CIP Cyber Security Standards, according to timelines specified in a separate table, following the identification and categorization of the affected BES Cyber System, with the additional time to comply for requirements in the same manner as those timelines specified in the section *Initial Performance of Certain Periodic Requirements* above.

Time Periods for Disaster Recovery

Several commenters requested clarity on what constitutes the completion of the Disaster Recovery. In response, the use of the defined term CIP Exceptional Circumstance throughout the CIP Cyber Security Standards eliminates the need to define a special case in the implementation plan for Disaster Recovery. Entities can take exceptions from the Requirements where CIP Exceptional Circumstances is specified.

One commenter suggested that the Disaster Recovery section seems to suggest not holding up restoration for compliance but entities would need to be compliant when restoration activities are complete. In response, this section

has been removed and we defer to the use of CIP Exceptional Circumstances throughout the CIP Cyber Security Standards to provide entities clarity on when and where exceptions to the Requirements can occur.

Applicability Reference Tables

One commenter requested additional clarification regarding the purpose of the applicability tables and others noted inconsistencies with the table. In response, we have corrected inconsistency errors, changed the title and provided introductory remarks. These tables are intended only for convenience. The SDT chose not to include this in a background or guidance section because requirement numbering will change in future revisions.

QUESTION D17 – DEFINITIONS AND IMPLEMENTATION PLAN:

If you have comments or specific suggestions that you have not been able to provide in response to the previous questions, please provide those comments here. Please provide specific suggestions or proposals for any alternative language.

SUMMARY:

Based on stakeholder comments, the implementation plan was modified appropriately and certain areas were modified for clarity. Entities should refer to the individual responses to comments in the definitions questions for the SDT's response to comments for individual definitions. Many commenters provided comments on the positive direction of the posted draft. The SDT thanks these commenters and appreciates the encouraging remarks.

Several comments were toward the approach to requirements that result in a zero tolerance aspect for deficiencies in compliance monitoring. The SDT has proposed additional language that, together with a framework that also includes VSL language and RSAW audit guidance language, addresses the larger issue and shifts the focus of certain requirements to correcting deficiencies. This is explained in greater detail in the summary explanation at the beginning of this document.

Several commenters expressed their concerns on the protection of Low Impact BES Cyber Systems and the compliance demonstration of requirements that apply to them. The SDT has spent considerable time and effort to work with stakeholders on addressing this issue and believes that the approach in the new proposed draft addresses the concerns.

Multiple commenters reiterated concerns on the broad application of CIP V5 irrespective of connectivity. The SDT has included consideration of connectivity in the applicability of requirements and believes that this approach appropriately addresses applicability differences due to connectivity type. The SDT reiterates its posture that, while connectivity is an important vector for cyber security threats, it is not the only one and that the CIP standards encompass a holistic approach to the protection of BES Cyber Systems.

There were multiple comments that suggested the phrase "but not limited to…" may be construed as required evidence. The SDT agrees with the comment and is using the standard language "Example(s) of evidence may include, but is not limited to…" to convey two concepts in the measure: the evidence in the measure are not required evidence but represents examples of quality evidence, and entities may present other evidence that may be presented in lieu of the ones described or in addition to them.

Multiple comments were based on the definition of periodic requirements, with another commenter citing the CAN on Annual that has been published. The SDT notes that CANs provide guidance for auditors, are not interpretations of standard requirements and are not the basis for changes to requirements. The SDT has considered all outstanding CANs as additional input to the development of these standards, and where the CANs result from unclear requirement language, the SDT has drafted language with a goal of eliminating the need of a CAN for auditing purposes. Since the word annual is not used in the V5 CIP standards, the term does not apply. The SDT has drafted language that reflects its intent while providing adequate flexibility to minimize zero defect effects.

Several commenters requested a global clarification similar to section 5 of CIP-003 that explains the significance of the use of bulleted and numbered items. Another comment was on the bullets in section 4, part 4.2.2. The SDT will insert a paragraph in the background section to include such explanations.

There were several comments on the use of a single VRF for each requirement, irrespective of whether it applies to High Impact or Medium Impact. Another comment was on the VSLs and the differentiation required to handle zero defect. VRFs are used as one of many input variables used to determine the sanction in the case of a violation of a standard. The current sanction table used for calculating regulatory sanctions is based on VRFs at a requirement level. However, there are many other considerations in the determination of a sanction for a specific violation. Until the current development of the evolving enforcement model is better defined, it is premature to effect changes to the VRF. Regarding VSLs, the SDT notes that VSLs are used after the fact, i.e. when a violation has already occurred. The SDT believes that VRFs, VSLs and RSAWs, together with appropriate requirement language, must together provide a complete framework to address the zero defect issue. The ballot for VRFs and VSLs is a non-binding ballot, and there is likely to be changes to accommodate evolving concepts in handling zero defect compliance and risk based compliance assessments.

Several comments were on the compliance section on records retention and retention requirements in standards requirements. Retention requirements, when specified in requirements, are requirements for technical reasons, such as event log retention for forensic purposes. The retention periods specified in the compliance section are meant to apply to records required for demonstrating compliance. For example, if 90 day event log retention is specifically required in a requirement, the Responsible Entity is expected to retain records that demonstrate that it has kept 90 days of logged events for the 3 years, not that it has kept 3 years' worth of these event logs. Under the compliance section, these could be log entries of the process that maintains a minimum of 90 days of log events.

Several commenters suggested that all sub-requirement parts should state the goal. The SDT generally provides the goal either in the body of the main text for the requirement, or in the rationale box. The SDT believes that the goal of each subpart is mostly self-evident given the overall requirement objective, and that addition of a goal for each subpart would be redundant and unnecessary in most cases.

There were several comments surrounding the need for a definition of Control Centers. The SDT directs entities to its summary response to Question D9 on this issue.

There were several comments on the removal of restoration resources from Medium Impact criteria, and cited the need to provide adequate justification. It is not clear to the SDT whether these comments were in support of this change. However, as a matter of normal SDT stakeholder input consideration, extensive debate on this issue was conducted in the NERC operating and planning technical committees, without a clear resolution. As a matter of procedure, the SDT must provide justification for changes from one release to another and has received stakeholder comments supporting this change.

There were multiple suggestions that a summary of the CIP Version 5 standards and the interaction between the requirements and their applicability be provided by the SDT. The SDT is focused on addressing technical issues from comments on requirements and on the standards themselves. The SDT appreciates any input provided by stakeholders, and it plans to facilitate distribution of an informational summary addressing this concern that was prepared by certain stakeholders that have been collaborating with the SDT. However, the formal posting with the standards would require other types of SDT, NERC and other stakeholder groups' review and/or approval and is not an appropriate venue for making compliance management tools available to stakeholders.

There were several comments on the issue of physical access controls for High Impact, specifically on whether two different access control systems are required. The SDT has provided guidance on this issue in the guidelines and technical basis section of CIP-006 that indicate that the intent of the requirements is not to require different control systems.

Numerous commenters expressed concern with the term "Associated Protected Cyber Assets". In considering these comments, the SDT noted that the concept of high water marking for Impact Level within an ESP was not very clear. The SDT has defined a term Protected Cyber Assets to incorporate the concept of BES Cyber Systems, their associated Cyber Assets within the same ESP and the concept of High Water Marking for Impact level within an ESP.

There were several comments that a definition for dial-up connectivity is needed. The SDT has included a definition for "Dial-up Connectivity" in this draft proposal.

There were comments on the use of "Associated…" in the applicability column of requirement tables. The SDT has made some changes to the language used to clarify the applicability and has also used the defined term Protected Cyber Assets to further clarify applicability.

There were comments relating to a number of editorial and stylistic issues related to table headers, capitalization and inconsistencies of terms. The SDT has considered these comments and made the appropriate changes.

One commenter recommended that the exemptions section in the applicability section should be specific to the standard, and not say CIP-002-5 in standards other than CIP-002. The SDT agrees and has made the appropriate changes in the standards.

One commenter suggested that the application guidelines should be allowed to change from standard to standard and that glossary terms should not be defined again in the standard. The SDT disagrees that application guidelines should be the same for all standards, but does agree that there should not be any incompatibility or inconsistency between the guidelines and the standards. The SDT also agrees that there should not be any definitions repeated in a standard when they are proposed glossary terms. The SDT will ensure consistency between guidelines and standard requirements. The SDT notes that the notes on glossary terms in the guidelines or background section are intended to provide additional explanantion of the terms and not be replacement definitions for the proposed terms for the NERC glossary. The requirements in the standard are the ultimate source of authoritative text for compliance.

One commenter suggested that the requirements that should be subject to CIP Exceptional Circumstances should be extended to most requirements except those in CIP-002, CIP-003 and CIP-004, and provided a list of requirements that should be subject to CIP Exceptional Circumstances. The SDT has carefully selected requirements that it believes are appropriately suitable for a CIP Exceptional Circumstance in order to facilitate the handling of emergency situations and timely electronic and physical access for first responders. With regard to a comment on ensuring that CIP Exceptional Circumstance would not require a TFE, the SDT has no jurisdiction over Rules of Procedure and cannot predict what regulators will deem to be TFE triggering language in the future. It is not the SDT's intent that CIP Exceptional Circumstances be TFE triggering language, but rather, that the Responsible Entity has carefully defined its policies and

procedures for declaring and ending CIP Exceptional Circumstances as required in CIP-003, and that any specific CIP Exceptional Circumstance be documented as required to demonstrate compliance to the specific CIP requirement.

One commenter suggested that it should be clear that no policies or procedures are required for CIP-004 to CIP-011 Responsible Entities that do not have High or Medium Impact BES Cyber Systems. There is no requirement in CIP-004 through CIP-011 that is applicable to Low Impact BES Cyber Systems. This is clear in the applicability column of the requirements tables.

There was a comment on the incorporation of guidelines and technical basis in the standards, citing stakeholders' time constraints in reviewing guidelines during the comment period. The SDT has spent considerable time drafting guidelines and providing the technical basis for requirements as part of the structure of results based standards. The SDT believes that the guidelines and technical basis provides valuable information to stakeholders during the comment and balloting process. It provides valuable input to stakeholders on the intent of the SDT, both during the development and the implementation phases of the standards. This approach has received overwhelmingly positive feedback from stakeholders. While the SDT understands that these guidelines and technical basis are not intended to be used instead of, or in addition to requirements, the SDT believes they provide valuable context to the standards' requirements.

There was one comment on the use of attestations as measures, citing industry confusion on the appropriate use of attestations. The absence of "attestations" in the measures does not imply that attestations are not appropriate measures of compliance, but that the SDT chose to use more specific examples of evidence for these requirements. Whether attestations are appropriate measures of compliance depends on the requirement. The SDT has used attestations where it may more likely be the measure that can be produced as evidence of compliance, with no implication that it is the only way of demonstrating compliance.

One commenter suggested that part 4.2.3 of the applicability section (Section 4) may inadvertently create an exemption for Control Centers. While certain Functional Entities may not own BES Facilities as described in the NERC Glossary, they perform reliability functions as the Functional Entity listed in 4.1 for BES Facilities. The introductory paragraph of 4.2 specifically refers to "…Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above …"

One commenter requested clarification or a definition of "Adverse Reliability Impact": this term is defined in the NERC Glossary of Terms.

One commenter requested a formal definition for “Common Control System”: the SDT believes that the term control system is a widely understood term of art used in electric reliability operation and engineering and that it does not require specific definition in these standards.

One comment suggested that the standards use data and information interchangeably. The SDT notes that it has used data when referring to a set of values (numeric or otherwise) in its raw form, and to information when referring to data processed for a specific use.

One commenter noted that the CIP standards should be aligned more closely to the NIST or ISO standards. The SDT uses many frameworks (including the ones cited) as sources for the development of requirements. The SDT notes that both of the cited standards are general purpose cyber security standards and guidelines not intended for any specific industry use. The SDT believes that the mandatory nature for standards specifically for the BES poses unique challenges and requires an appropriately developed approach.

There was one comment that was extensively on the scope of applicability to asset owners and operators only, and the absence of compliance for suppliers and other third party providers. The SDT notes that these mandatory standards are developed under the jurisdiction of the ERO and that they can only be applied to NERC Registered Entities.

One comment was on the awareness and training requirement in CIP-004 R2 and role based awareness training. The comment was specific that the items in the table in R2 referred to systems while the requirement cited role based training. Table R2 contains the requirements for the required content of the training program, but the level at which the training is provided in each item is based on the role of the individual taking the training.

One comment was extensively on the 99.9% availability specification in CIP-006. The SDT has redrafted the requirement and the 99.9% specification has been removed.

There was one comment on the effect of the application of the CIP standards on small entities. The SDT notes that BES Cyber Systems are categorized based on reliability impact rather than on entity size. The SDT has developed the requirements to be commensurate with the level of impact on the BES. The SDT has not included entity size as an input to the applicability of requirements.

One comment was extensively on section 4.2.2. The SDT notes that section 4.2.2 is not intended to specify the impact criteria, but the scope. Consequently, many of the terms used are extracted from the registration criteria for DPs. Many of the comments presented have been incorporated in the proposed new draft, while a few are appropriate as part of the criteria.

One commenter made many remarks on global sections used in all standards. These will be reviewed by NERC standard staff as standard templates applicable to NERC standards.

There was a comment on the use of "where technically feasible" and the commenter suggested the use of language that would specify compensating controls. The SDT notes that there were requirements in CIP Versions 1-4 that had alternative language to allow compensating controls, but that the language was added to TFE triggers.

One commenter requested a definition of "Associated Data Centers". Please refer to the summary response on this issue to comments on D9.

One commenter was concerned with the periodic requirements, specifically on the 15 month period for periodic requirements intended to be performed annually. The commenters suggested alternative language that would ensure strict compliance with a 12 month period. The intent of the SDT in specifying a 15 month period for annual requirements is to provide some flexibility to entities in the framework of attenuating zero defect requirements. The comments imply that Responsible Entities would aim for strict minimum compliance at the cost of increased non-compliance risk. From the practical implementation standpoint, the SDT understands that most Responsible Entities will implement a process that would ensure the performance in a period less than 15 months (an annual period is easier to track from the compliance management standpoint) for assured compliance.

One comment was raised on the SDT's discussion of redundancy as not being a mitigation for cyber security vulnerabilities and stated that redundancy provide mitigation for some cyber security vulnerabilities. While redundancy provides some mitigation for recovery requirements, the SDT has not found a compelling case where strict redundancy of using an exactly mirrored system configuration would provide mitigation of a cyber security vulnerability. It is the SDT's opinion that such configurations have the unintended effect, from the cyber security (not operational) standpoint, of increasing the attack surface. The SDT does agree that configurations that provide redundancy of function rather than system redundancy can provide mitigation if implemented with systems dissimilar enough to provide mitigation of certain system specific cyber security vulnerabilities.

One comment was on the term Facility and its relation to systems, also stating that the term element is undefined. The SDT has used the term Facility in its defined meaning in the NERC Glossary when used in its capitalized form. The term Facility is used to refer to groups physical BES Elements. The NERC Glossary has a definition of Element used in the context of the BES. In cases where the SDT intends a broader scope to include systems, the SDT has used "Facilities, systems and equipment".

There was a comment on the exemption from the standards of cyber assets between discrete ESPs. In particular, the commenter suggested requirements to implement end-to-end encryption. The commenter seems to suggest that such encryption should be required for routable and non-routable protocols. In addition, the commenters suggest that EAPs should be subject to cyber security requirements. The SDT has not required specific technologies to protect information between ESPs, but has focused instead on the cyber security objectives of access control and monitoring of traffic across EAPs. The comments do not seem to take into account communication between ESPs of real-time, latency sensitive applications common in control systems. The authenticity and integrity of application data or information is not always implemented using communication encryption technology, but may be implemented at other layers of the overall stack without the latency overhead of encryption. The commenters also seem to interchangeably use EAPs and the cyber assets that implement the EAP. The CIP definition of an EAP is an interface. There are however requirements, including security event monitoring requirements, that are applicable to the Cyber Assets that perform access control and monitoring functions, including those that implement an EAP, for electronic and physical access.

A commenter suggested that BES information protection requirements should apply to third parties. The SDT agrees and expects the Responsible Entity to comply with requirements for protecting and handling BES protected information, whether such information is accessed or handled by its own employees and third parties. The requirements in CIP-011 require the Responsible Entity to implement processes to ensure such access control and handling.

One commenter provided its fundamental objection to Version 5 and suggested that implementation of the current CIP standards should be allowed to mature. The SDT is required to address all the FERC directives from Order 706, and FERC Order 706 has directed the ERO to complete consideration of Order 706 directives by March 31st, 2013.

One commenter suggested that the statement in the implementation plan that starts with "Not withstanding any order to the contrary…" should be amended in light of Order 706. The SDT believes that the window for the application of the statement is still possible given the deadline in Order 761.

One commenter inquired on when a cyber system would have to come into compliance as a result of an emergency. One commenter also inquired on how to treat temporary elevation. If the cyber system is re-categorized or is a new cyber system as a result of that emergency or unplanned change, the implementation table specifies 12 months.

There was a comment on missing requirements in item 5 of the Implementation Plan. The SDT has included these requirements.

One commenter pointed out that the background section dealing with reliable operation of the BES contains an unclear reference to the Functional Model. The SDT has added qualifications that clarify that both reliability tasks defined in the Functional Model and the functional entity's relationships with other functional entities are considered.

One commenter suggested that there are requirements where the text of the requirement specifies BES Cyber Systems when the applicability column specifies more than BES Cyber Systems. The SDT has reviewed the language of the requirements where this occurs to ensure consistency with the applicability column. In cases where more than BES Cyber Systems apply, the SDT generally uses "applicable Cyber Assets."

One commenter expressed the need for the concept of escorted electronic access for remote support using technologies such as WebEx. The fundamental concept in escorted access is not only that of continuous visibility on the actions of the escorted individual, but also the capability of timely intervention in the case of inappropriate action. The SDT believes that total support for this concept is not possible in an electronic access scenario.

One commenter stated that in its opinion, the functional entity Interchange Coordinator (IC) does not have any asset that would be included, and should therefore not be included in the applicability section. The SDT reviewed the reliability tasks for the IC function as well as the responsibilities of the IC Functional Entity in its relationship with other functional entities in the Functional Model and noted real-time responsibilities in the latter in relation to BAs and RCs.

Questions with Votes Only:

1. Do you agree with the proposed definitions of BES Cyber Asset, BES Cyber System, and Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
FirstEnergy	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No

Organization	Yes or No
ACES Power Marketing	No
SPP and Member companies	No
Comment Development SME List	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Hydro One	No
Ingleside Cogeneration LP	No
NIPSCO	No
Trans Bay Cable	No
Consumers Energy Company	No
Bonneville Power Administration	No
Snohomish County PUD	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	No
American Transmission Company, LLC	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
ISO New England Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No

Organization	Yes or No
Deseret Power	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
US Bureau of Reclamation	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
IRC Standards Review Committee	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes

Organization	Yes or No
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes

Organization	Yes or No
Turlock Irrigation District	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Pacific Gas and Electric Company	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes

2. Do you agree with the proposed definition of Control Center?

Organization	Yes or No
NRG Energy Companies	No
PNGC Comment Group	No
Madison Gas and Electric Company	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
NCEMC	No
ACES Power Marketing	No
IRC Standards Review Committee	No
National Rural Electric Cooperative Association (NRECA)	No
Southern California Edison	No

Organization	Yes or No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
PSEG	No
Texas Reliability Entity	No
Liberty Electric Power LLC	No
PJM Interconnection	No
City of Austin dba Austin Energy	No

Organization	Yes or No
POrtland General Electric	No
Exelon Corporation and its affiliates	No
Farmington Electric Utility System	No
Indiana Municipal Power Agency	No
Deseret Power	No
Central Lincoln	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes

Organization	Yes or No
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
SPP and Member companies	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Dairyland Power Cooperative	Yes
Progress Energy	Yes
Western Area Power Administration	Yes

Organization	Yes or No
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes

Organization	Yes or No
United Illuminating company	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
Nebraska Public Power District	Yes
Utility Services Inc.	Yes
Alliant Energy	Yes
American Public Power Association	Yes

Organization	Yes or No
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes

3. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Dominion	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
NCEMC	No
ACES Power Marketing	No
Southern Company Services, Inc.	No
National Rural Electric	No

Organization	Yes or No
Cooperative Association (NRECA)	
Dairyland Power Cooperative	No
Tri-State G&T - Transmission	No
CenterPoint Energy	No
Manitoba Hydro	No
Xcel Energy	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
NextEra Energy, Inc.	No
Liberty Electric Power LLC	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Deseret Power	No
Brazos Electric Power Cooperative	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

4. Do you agree with the proposed definitions of BES Cyber System Information, CIP Exceptional Circumstances, and CIP Senior Manager?

Organization	Yes or No
Southwest Power Pool Regional Entity	No
Madison Gas and Electric Company	No
MRO NSRF	No
Duke Energy	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Southern Company Services, Inc.	No
Dairyland Power Cooperative	No
CenterPoint Energy	No
Trans Bay Cable	No
Manitoba Hydro	No

Organization	Yes or No
Snohomish County PUD	No
Lakeland Electric	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
Ameren	No
NextEra Energy, Inc.	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No
Alliant Energy	No
Exelon Corporation and its affiliates	No
California Independent System Operator	No
Northeast Power Coordinating Council	Yes
NRG Energy Companies	Yes

Organization	Yes or No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes

Organization	Yes or No
Salt River Project	Yes
Southern California Edison	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
NIPSCO	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Consumers Energy Company	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Bonneville Power Administration	Yes
Tampa Electric Company	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes

Organization	Yes or No
ISO New England Inc.	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes

Organization	Yes or No
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

5. Do you agree with the proposed definitions of Electronic Access Control or Monitoring Systems, Interactive Remote Access, and Intermediate Device?

Organization	Yes or No
Salt River Project	No
Trans Bay Cable	No
United Illuminating company	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Dairyland Power Cooperative	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
Oncor Electric Delivery Company LLC	No
Madison Gas and Electric Company	No

Organization	Yes or No
MRO NSRF	No
Duke Energy	No
Florida Municipal Power Agency	No
ACES Power Marketing	No
IRC Standards Review Committee	No
Comment Development SME List	No
CenterPoint Energy	No
NIPSCO	No
Bonneville Power Administration	No
MidAmerican Energy Company	No
Ameren	No
City of Austin dba Austin Energy	No
Nebraska Public Power District	No

Organization	Yes or No
Alliant Energy	No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
Brazos Electric Power Cooperative	No
Kansas City Power & Light	No
California Independent System Operator	No
Southern California Edison	Yes
ATCO Electric	Yes
Northeast Power Coordinating Council	Yes
Southwest Power Pool Regional Entity	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC	Yes

Organization	Yes or No
Registered Affiliates	
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
FirstEnergy	Yes
NCEMC	Yes
SPP and Member companies	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Hydro One	Yes
Clallam County PUD No.1	Yes

Organization	Yes or No
Ingleside Cogeneration LP	Yes
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
NV Energy	Yes

Organization	Yes or No
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
ISO New England Inc.	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
New York Power Authority	Yes
Farmington Electric Utility System	Yes

Organization	Yes or No
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
NYISO	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
US Bureau of Reclamation	Yes
Luminant	
American Transmission Company, LLC	

6. Do you agree with the proposed definitions of Electronic Access Point, Electronic Security Perimeter, External Routable Connectivity, and Protected Cyber Asset?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
MRO NSRF	No
FirstEnergy	No
Duke Energy	No
Florida Municipal Power Agency	No
SPP and Member companies	No
IRC Standards Review Committee	No

Organization	Yes or No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
NIPSCO	No
Hydro-QuÃ©bec Production	No
Turlock Irrigation District	No
Bonneville Power Administration	No
Lakeland Electric	No
Illinois Municipal Electric Agency	No
NV Energy	No
NextEra Energy, Inc.	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No

Organization	Yes or No
Exelon Corporation and its affiliates	No
Wiscsonsin Electric Power Company	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
NCEMC	Yes
ACES Power Marketing	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
CenterPoint Energy	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes
Independent Electricity System Operator	Yes

Organization	Yes or No
Trans Bay Cable	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Xcel Energy	Yes
Snohomish County PUD	Yes
Tampa Electric Company	Yes
MidAmerican Energy Company	Yes
Massachusetts Municipal	Yes

Organization	Yes or No
Wholesale Electric Company	
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Utility Services Inc.	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Farmington Electric Utility	Yes

Organization	Yes or No
System	
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

7. Do you agree with the proposed definitions of Cyber Security Incident and Reportable Cyber Security Incident?

Organization	Yes or No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
NRG Energy Companies	No
Madison Gas and Electric Company	No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Duke Energy	No
Family Of Companies (FOC) including OPC, GTC & GSOC	No
Texas RE NERC Standards Review Subcommittee	No
Florida Municipal Power Agency	No
Progress Energy	No

Organization	Yes or No
CenterPoint Energy	No
Hydro One	No
NIPSCO	No
Lower Colorado River Authority	No
LCRA Transmission Services Corporation	No
Xcel Energy	No
Bonneville Power Administration	No
Lakeland Electric	No
Tampa Electric Company	No
MidAmerican Energy Company	No
Illinois Municipal Electric Agency	No
NextEra Energy, Inc.	No
ISO New England Inc.	No

Organization	Yes or No
City of Austin dba Austin Energy	No
Utility Services Inc.	No
New York Power Authority	No
Farmington Electric Utility System	No
City Utilities of Springfield, MO	No
NYISO	No
California Independent System Operator	No
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
MRO NSRF	Yes
Dominion	Yes
FirstEnergy	Yes
NCEMC	Yes

Organization	Yes or No
ACES Power Marketing	Yes
SPP and Member companies	Yes
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Southern Company Services, Inc.	Yes
Salt River Project	Yes
Southern California Edison	Yes
Dairyland Power Cooperative	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
Ingleside Cogeneration LP	Yes

Organization	Yes or No
Hydro-QuÃ©bec Production	Yes
Independent Electricity System Operator	Yes
Trans Bay Cable	Yes
ATCO Electric	Yes
Consumers Energy Company	Yes
Manitoba Hydro	Yes
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
United Illuminating company	Yes
Turlock Irrigation District	Yes
Snohomish County PUD	Yes
NV Energy	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Tennessee Valley Authority	Yes

Organization	Yes or No
Ameren	Yes
PSEG	Yes
Texas Reliability Entity	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
Nebraska Public Power District	Yes
Alliant Energy	Yes
American Public Power Association	Yes
Springfield Utility Board	Yes
Exelon Corporation and its affiliates	Yes
Wiscsonsin Electric Power Company	Yes

Organization	Yes or No
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
Brazos Electric Power Cooperative	Yes
Kansas City Power & Light	Yes
US Bureau of Reclamation	Yes

15. Do you agree with the changes made to the proposed implementation plan since the last formal comment period?

Organization	Yes or No
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)	No
Southern California Edison	No
Dairyland Power Cooperative	No
Hydro One	No
Trans Bay Cable	No
Turlock Irrigation District	No
NextEra Energy, Inc.	No
Northeast Power Coordinating Council	No
Southwest Power Pool Regional Entity	No
MRO NSRF	No
NESCOR/NESCO	No
Duke Energy	No

Organization	Yes or No
Southern Company Services, Inc.	No
CenterPoint Energy	No
Consumers Energy Company	No
Manitoba Hydro	No
Snohomish County PUD	No
MidAmerican Energy Company	No
ISO New England Inc.	No
Nebraska Public Power District	No
Alliant Energy	No
New York Power Authority	No
Exelon Corporation and its affiliates	No
NYISO	No
Kansas City Power & Light	No
Texas RE NERC Standards Review Subcommittee	Yes

Organization	Yes or No
United Illuminating company	Yes
Massachusetts Municipal Wholesale Electric Company	Yes
Brazos Electric Power Cooperative	Yes
Utility Services Inc.	Yes
NRG Energy Companies	Yes
PNGC Comment Group	Yes
PPL Corporation NERC Registered Affiliates	Yes
Dominion	Yes
Family Of Companies (FOC) including OPC, GTC & GSOC	Yes
Florida Municipal Power Agency	Yes
NCEMC	Yes
ACES Power Marketing	Yes
SPP and Member companies	Yes

Organization	Yes or No
IRC Standards Review Committee	Yes
Comment Development SME List	Yes
Arizona Public Service Company	Yes
Progress Energy	Yes
Western Area Power Administration	Yes
Tri-State G&T - Transmission	Yes
Clallam County PUD No.1	Yes
NIPSCO	Yes
Independent Electricity System Operator	Yes
Lower Colorado River Authority	Yes
ATCO Electric	Yes
LCRA Transmission Services Corporation	Yes

Organization	Yes or No
Niagara Mohawk (dba National Grid)	Yes
National Grid	Yes
Xcel Energy	Yes
Bonneville Power Administration	Yes
Lakeland Electric	Yes
Tampa Electric Company	Yes
Illinois Municipal Electric Agency	Yes
NV Energy	Yes
Tennessee Valley Authority	Yes
Ameren	Yes
PSEG	Yes
Liberty Electric Power LLC	Yes
PJM Interconnection	Yes
City of Austin dba Austin Energy	Yes

Organization	Yes or No
Oncor Electric Delivery Company LLC	Yes
MEAG Power	Yes
POrtland General Electric	Yes
American Public Power Association	Yes
Wiscsonsin Electric Power Company	Yes
Farmington Electric Utility System	Yes
City Utilities of Springfield, MO	Yes
Pacific Gas and Electric Company	Yes
Deseret Power	Yes
Central Lincoln	Yes
Cowlitz County PUD	Yes
California Independent System Operator	Yes

Organization	Yes or No
Madison Gas and Electric Company	
Luminant	
American Transmission Company, LLC	

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments Cyber Security Order 706 Version 5 CIP Standards

Comment Form
Combined Question 1 and Question 2 Summaries
October 26, 2012

The Project 2008-06 Drafting Team thanks all commenters who submitted comments on the Version 5 of the CIP Cyber Security Standards and its Implementation Plan for consideration by the SDT in finalizing Version 5 and related documents. The 10 standards were posted for a 30-day formal comment period from September 11, 2012 through October 10, 2012 and successive ballots through October 10, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 112 sets of comments, including comments from approximately 258 different people from approximately 153 companies representing 9 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

Table of Contents

Introduction

The Standard Drafting Team (SDT) thanks all commenters for their continued focus on providing constructive and useful feedback for improving and refining the standards. In response to draft 3 of the Version 5 CIP Cyber Security Standards, the SDT received input that was focused on several issues that assisted the SDT in refining the standards to the final set of standards now posted for recirculation ballot. The SDT carefully considered all comments in determining whether to make particular changes to the standards.

In response to comments provided to draft 3, the drafting team greatly appreciates those entities that focused their comments on the issues most critical to them, as it facilitated a qualitative representative assessment of the areas requiring the greatest review. The focus on those major concerns that were essential as a condition to find consensus was greatly appreciated.

Furthermore, the SDT wishes to thank the industry for their significant engagement and support in developing these standards. Industry participants and observers, whether formally or informally, and whether in person or through other means, provided important perspectives and subject matter expertise that facilitated the SDT's consideration of the complicated issues and technical matters reflected in these standards. This truly was a collaborative process with participation from virtually every facet of our diverse and committed industry. Security and reliability were reflected in each consideration, and the extensive and consistent industry participation throughout the process is reflected in high approvals in response to the successive ballot from draft 3 that ended October 10, 2012.

At this stage, the drafting team has reached a point where it has made a good faith effort at resolving applicable objections, and it has not made any substantive changes since posting draft 3. Therefore, the team is posting the standards, related definitions and implementation plan for a recirculation ballot. As in past drafts of the Version 5 CIP Cyber Security Standards, the SDT thoroughly considered proposed changes and evaluated them carefully by considering several important variables, such as, but not limited to, whether such changes were in the interest of cyber security and reliability, whether they would improve or reduce consensus, whether they had unintended consequences for other types of entities, and whether they were in support of the SDT's obligation to respond to regulatory directives, most notably from FERC Order No. 706. The SDT has done its best to be responsive to all inputs, recognizing that it is not possible to adopt every suggestion and also recognizing the considerable diversity of entities and assets to which the standards will apply.

In the accompanying comment form for draft 3, the drafting team asked the following two questions:

1. If, after reviewing the posted standards and General Summary of Consideration of Comments, you do not support one or more of the 10 standards, the implementation plan or set of definitions, please indicate the specific item you do not support (the standard and Requirement number, specific defined term, or implementation plan) and the specific reason you cannot support it here.
2. If you have a brief comment you would like to provide that has not already been provided among the previously submitted feedback in response to draft 1 and draft 2, please provide it here. Please limit your comment to 200 words or less.

In reviewing comments, the SDT determined that some common issues were presented by different entities in response to either Question 1 or Question 2, depending on how the particular entity organized its comments. As a whole, the SDT found that the responses were thoughtful, organized, and focused. In this summary, the SDT is responding to all comments from industry that were submitted in response to both Question 1 and Question 2 in one consolidated summary form rather than providing a separate summary for each of Question 1 and Question 2. Since most issues and comments were not isolated in response to one question or the other, this single summary provides the most efficient and thorough method with which to provide the SDT's response.

Commenters addressed a wide variety of topics in their comments, but the most commented upon subjects include comments on the Transmission Operator (TOP) Control Center Criterion in CIP-002-5's Attachment 1 and comments regarding the SDT's use of the "in a manner that identifies, assesses, and corrects deficiencies" language. The TOP topic is discussed in detail under the CIP-002-5 portion of this summary, and the "identifies, assesses, and corrects deficiencies" topic is addressed immediately below as part of this summary's general discussion. Other topics are discussed relative to their particular standard or definition, and the associated table of contents for this document lists most topics of discussion.

"Identifies, Assesses, and Corrects Deficiencies" Comments

As noted in the background sections of the standards, and in response to comments from draft 2, the SDT has incorporated within CIP Version 5 a recognition that certain Requirements should not focus on individual instances of failure as a sole basis for violating the standard. In particular, the SDT has incorporated an approach to empower and enable the industry to identify, assess, and correct deficiencies in the implementation of certain Requirements. The intent is to change the basis of a violation in those Requirements so that they are not focused on *whether* there is a

deficiency, but on identifying, assessing, and correcting deficiencies. Note that, where used, the addition of language modifies "implement"; it does not itself require or specify internal controls, though it certainly enables their use for those entities that have adopted an internal controls or compliance management approach. For purposes of this summary, the "identifies, assesses, and corrects deficiencies" phrase is sometimes referenced as simply "IAC."

This topic was a source of several comments on draft 3, and the SDT appreciates the comments, feedback, and the spectrum of concern or support on this issue. The SDT believes that Version 5 is the right time to take a step in a direction that promotes security and reliability by incorporating a self-correcting aspect in certain Requirements. This is a new step, but it is informed, collectively, by implementation and audit experience from Versions 1 through 3 of the CIP Cyber Security Standards.

Many commenters support the SDT's addition of a self-correcting aspect and applaud the overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. The commenters support the shift from zero tolerance for deficiencies to encouraging finding and correcting deficiencies. The SDT considers such self-correction as an essential component to improved reliability and security, and it thanks commenters for their support. Though there were several specific suggestions or concerns, as noted below, the consensus position of the industry is one of support for the approach, as reflected in both comments and the overwhelming approval of the standards that use the approach.

While this is a new direction, the SDT believes there is tremendous benefit in eliminating the zero-defect language in the standards, and it is therefore worthwhile of inclusion in the CIP standards. However, the SDT acknowledges this is a developing concept and encourages the industry to continue to work alongside NERC in implementing the compliance monitoring strategy for the language.

Some commenters presented concern that there is no clear mechanism with how this approach will be audited or that there may be inconsistent audits across Regions. The SDT is well aware of this concern, and it is encouraged by ongoing coordination and support among both NERC and several regions. The SDT expects that NERC will continue to develop tools such as the Reliability Standard Audit Worksheets (RSAWs) in a manner that involves the industry and the members of the SDT. Importantly, the language to "identify, assess, and correct deficiencies" modifies "implement" where used, and it is meant simply to express that implementation of the Requirement is not in a "zero defect" manner.

Commenters also questioned whether this approach indeed does require internal controls. The SDT notes that the compliance initiatives that relate to internal controls are not the same as the approach in the standard. The SDT contemplates that the "identify, assess, and correct deficiencies" language is appropriate regardless of how compliance may be monitored, while noting that the standards approach is also supportive of the compliance approach where and if used. At its core, the SDT intends in using the language to signal an important transition to self-correction as part of the expected performance of a Requirement itself as opposed to a mere deficiency constituting the basis for violation.

Some commenters also proposed alternative, additional, or supporting language to augment the "identify, assess, and correct deficiencies" language in the Requirements or other supporting components of the standards, or proposed addition of the language to other requirements. The SDT has previously considered such alternative language and evaluated carefully where the language should be used, and, upon reexamining those proposals in response to comments, the SDT continues to support those concepts in the compliance monitoring approach and documents rather than in the standards themselves. Language noting that certain actions are not violations is too prescriptive for either the Requirements or the measures, and they do not comport with the style and form of the standards. With continuing input, coordination, and education, the SDT is confident that the Requirement language as presented is the appropriate mechanism to empower the industry to focus on correcting deficiencies as part of the expected performance of the Requirements while not requiring or prescribing a particular assessment of the how the entity accomplishes it.

Additionally, in response to perspectives expressed by commenters on the "identify, assess, and correct" deficiencies language, the SDT shares the view that NERC must ensure going forward that the compliance monitoring approach is consistent. The SDT believes that most of the industry is ready to transition to a new approach and that this reflects the consensus position. The SDT and the industry have an opportunity to incorporate significant improvements and lessons learned from implementation and audit of previous versions, and the SDT is encouraged by not only industry support, but also from NERC's direction in continuing to work with the industry in implementation of risk-based initiatives. The SDT will remain engaged after approval of the standards to work with NERC to provide input into the RSAW development process.

Section 4 - Applicability

There were many comments that "group of Elements" from the standards' applicability section, parts 4.1.2.4 and 4.2.1.4 should be deleted on the bases that it is redundant with Cranking Path and would create ambiguity, citing that these and initial switching Requirements are included in the Cranking Path. The SDT considered the language that is included in Requirement R1.5 of EOP-005-2, which says: "Identification of Cranking Paths and initial switching Requirements

between each Blackstart Resource and the unit(s) to be started." The addition of the term "group of Elements" is based on this Requirement that includes "and initial switching Requirements" in addition to the Cranking Path, and it is meant to include the group of Elements that is included in these initial switching Requirements.

One commenter requested clarification on the applicability of Section 4 with respect to Distribution Providers (DPs). The SDT notes that the clarification is included in the Guidelines and Technical Basis section of the standards relating to applicability. The guidance specifically says: "Note that there is a qualification in section 4.1 that restricts the applicability in the case of Distribution Providers to only those that own certain types of systems and equipment listed in 4.2." This means that DPs that own assets listed in 4.2 are subject to the standard. In addition, "For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above" are excluded from applicability of the CIP standards. That means that only systems and equipment listed in 4.2.1 are subject to the CIP Cyber Security standards.

Many commenters stated that the qualifications for applicable assets in section 4 for Cranking Paths unfairly includes non-BES facilities for DPs while excluding those from Transmission Owners (TOs) and TOPs, for which all BES Facilities are defined under section 4 as applicable. Alternate language was proposed to only include BES facilities in the scope for Cranking Paths. The SDT clarifies that those TOs that own BES Facilities as well as non-BES facilities that are qualified for DPs will also be registered as DPs. A review of the registry listing from September, 2012 showed that 232 of the 340 registered TOs (68%) are also registered as DPs. The SDT further points out that the inclusion of DPs in the applicability ensures that non-BES facilities, such as those that support the restoration of the BES, that are impactful to the reliability and operability of the BES are included.

One comment read that it appears that small entities that own stand-alone UFLS systems with no communication facilities would have applicable Requirements under these standards. It is the intent of the SDT to include all UFLS systems that meet the criteria defined in section 4. These criteria do not include any exclusion based on connectivity. The SDT points out that for DPs, only those UFLS systems that can automatically shed 300 MW or more under a common control system are qualified for applicability. The Requirements that are applicable based on connectivity are specified in CIP-003 through CIP-011. The commenter also stated that, "Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system." The SDT clarifies that the owner of all qualified cyber systems is the entity responsible for compliance of these cyber systems: while the common control system that is capable of shedding 300 MW qualifies that UFLS, all cyber systems that impact the reliable operation of the UFLS system become in scope. The

responsibility for the compliance of each of these cyber systems to applicable Requirements belongs to the owner of that cyber system.

One commenter stated that the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for DPs to include facilities containing "A Protection System that applies to Transmission ..." is a new (initially introduced in draft 2) unsubstantiated Requirement for low impact assets. The SDT points out that among the tasks of the DP in the Functional Model is to "design and maintain protective relaying systems, under-frequency Load shedding systems, under-voltage Load shedding systems, and Special Protection Systems that interface with the transmission system." Further, the NERC Statement of Compliance Registry Criteria (Appendix 5B of the NERC Rules of Procedure) includes:

> "III.b.2 Distribution Provider is the responsible entity that owns, controls, or operates Facilities that are part of any of the following Protection Systems or programs designed, installed, and operated for the protection of the Bulk Power System:
>
> - a required UFLS program.
> - a required UVLS program.
> - a required Special Protection System.
> - a required transmission Protection System."

The same commenter suggested that the inclusion of all BES Facilities in section 4 is excessive. The SDT takes the position that cyber systems that impact the real-time operation of any BES Facility must be subject to some form of protection that is commensurate with its impact. The SDT points out that only those BES Cyber Systems that have a real-time impact to the BES are included by definition. This is also in consideration of comments in FERC Order No. 761.

Another commenter wrote that the use of the defined term "BES Facilities" in the applicability section would exclude such assets as Control Centers and Protection Systems. While these facilities are not BES Facilities per se, they are facilities essential to the reliable operation of the applicable BES Facilities and are included for applicability because of the function they are providing for reliable operation of BES Facilities.

One commenter stated that the clause "is subject to one or more Requirements in a NERC or Regional Reliability Standard" was unclear and proposed "can affect the reliability of either Medium or High Impact Facilities." The SDT believes that DPs have to comply with NERC Reliability Standards for some facilities they own and that the current clause

provides certainty as to what those facilities are since these DPs are required to comply with these standards. The SDT feels that the proposed language provides less certainty and is more subjective.

One commenter noted that exempting utility owned communications infrastructure (exemption of communications facilities between ESPs) creates a cyber security issue. The SDT believes that utility owned carrier services should be treated in exactly the same way a third party carrier is viewed in terms of trust, and that adequate protection measures should be taken to protect against an untrusted (from the BES Cyber System point of view) service provider.

Draft Reliability Standard Audit Worksheet

Some commenters provided input and feedback in their comments to the draft RSAW for CIP-006-5 that NERC Compliance Operations posted concurrently with draft 3 of the CIP Cyber Security Standards. The intent of the SDT in contributing to the development of a draft RSAW for CIP-006-5 was to begin the initiative of developing RSAWs in concurrence with standard development projects. The SDT provided input to the draft of the RSAW, and it is encouraged by the opportunity for the SDT and industry to continue to provide input as the RSAWs continue to be developed subsequent to the industry's approval of these standards. The SDT has forwarded these constructive inputs to NERC Compliance Operations for their continuing consideration.

"Annual" and Other Time Parameters

Some commenters pointed out that in a few instances, the SDT inadvertently continued to use the "at least once each calendar year (or similar)" language in conjunction with the convention to not exceed 15 calendar months. The SDT has reviewed the standards and eliminated those "calendar year" references where the SDT intended to use only the phrase "at least once every 15 calendar months."

A few commenters continued to suggest alternatives or expressed preference for retaining only the "annual" reference, which would result in continued reliance on CAN-0010. The SDT has not implemented that change because within Version 5 there is an opportunity and an obligation to unambiguously reference the periodic time parameter. The SDT also explained this in greater detail in response to draft 2 of the Version 5 CIP Cyber Security Standards on pages six and seven of summary consideration of comment form A.

One commenter expressed a desire to adopt a "once per month" convention instead of using, "At least once every 35 calendar days..." where that phrase is used. This is similar to the discussion on "annual," and for similar reasons, the SDT has not made the change. The SDT intends for these time periods to be repeatable on a basis that approximates

performance on the same day per month, or more frequently. The SDT believes it is reasonable to use 35 calendar days to account for those scenarios where a month may begin or end on a weekend, or for holidays.

Authorized Access List and Specific Rights Reviews in Multiple Standards

One commenter identified possible issues with a lack of understanding and inconsistent implementation for authorized access lists and specific rights review in Versions 1 through 3 of CIP-004 Requirement R4, CIP-003 Requirement R5, and CIP-007 Requirement R5. The commenter further stated that there was a concern that the quarterly and annual verification of CIP-004-5 Requirements Parts 4.2 and 4.3 are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve existing issues.

Similarly to the comment above, another commenter had issues with a lack of understanding and an inconsistent implementation for authorized access list and specifics rights review with the multiple standards as mentioned in the previous paragraph. The commenter was concerned that CIP-004-5 Requirement Parts 4.2 and 4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. Furthermore, the commenter stated that access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated Requirements. In response to the two aforementioned comment responses, the SDT has modified Requirement Parts 4.2 through 4.5 to state up front to which type of access each Requirement Part applies. CIP-007-5 Requirement Part 5.2 is a security hardening control applying to the enabling or disabling of generic accounts (From the Technical Guidelines section: A generic account is a group account set up by the operating system or application to perform specific operations. This differs from a shared user account in that individual users do not receive authorization for access to this account type).

The key distinction between CIP-007-5 Requirement Part 5.2 and CIP-004-5 Requirement Part 4.3 it that generic accounts and associated privileges are not authorized nor is there the same concept of "need to know." CIP-004-5 Requirement Part 4.3 applies to user accounts only and would not necessarily indicate a full listing of user accounts and privileges on the system. However, one could envision a process by which an entity finds it more efficient to perform a full account listing and thereby produce evidence in compliance for both Requirement Parts. The SDT also point out that the identification of default or generic accounts occurs only once and does not require annual verification.

The SDT acknowledges the listing of individuals with authorized access to shared accounts (CIP-007-5 Requirement Part 5.3) has a connection to the authorization of CIP-004-5 Requirement R4 because entities must know the list of individuals

authorized to a shared account in order to fully perform the quarterly and annual assessments. However, entities may comply with the Requirement to authorize access to a BES Cyber System without specifying how they obtain such access. Overall, the SDT sees valid arguments for this Requirement Part residing in both CIP-004-5 and CIP-007-5. Because of the history of prior versions, the difference in applicability, and the significance in moving a Requirement Part to a different standard, the SDT choose to retain the Requirement in its original location.

Data Retention Requirements

There were several commenters that stated specifically and in general to exclude any data retention Requirements from the standard. In response, these few Requirements are not intended to specify a retention period as done in the Compliance section of standards, but to retain information for the purpose of incident response and analysis.

CIP-002-5

Draft 3 of CIP-002-5 obtained an affirmative ballot result of 74.9% with a quorum of 80.6% of the ballot pool at its successive ballot of October 2012. This result indicates a very significant improvement from the previous ballot and achieves a high level of stakeholder consensus.

One commenter noted an inconsistency in sub-Requirement numbering in the standard. This has been corrected and the part numbers have been changed in CIP-002-5 to remove the "R" from Requirement "R1.1", etc., to "1.1", etc.

There was a comment that stated the purpose of the standard is inconsistent with the approach, further noting that "the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System." The SDT notes that the standard has taken the approach that the categorization of qualified BES Cyber Systems is based on the impact of the functions performed by the assets they are supporting. This is consistent with risk management approaches that evaluate risks based on the functional objective of the organization (in this case the reliable operation of the BES). The same entity proposed a multilevel evaluation of the impact of cyber systems based on functional impact as well as the individual impact of the cyber system within the functional impact. This multilevel approach was one that was proposed to stakeholders early in the development process: industry comments called for a simpler approach which resulted in the current one.

Another commenter stated that the CIP-002-4 and Version 5 "bright-line criteria" step away from a risk based method to a prescriptive approach. The commenter further wrote that it is an inverted philosophy from the approach draft 3 used in the other CIP Version 5 standards. The SDT notes that CIP-002-5 follows on the approach used in Version 4, which has been approved by the industry and by FERC, for using bright lines instead of an entity-defined risk-based methodology for evaluating the impact of assets, and the SDT is extending the concept with a multi-tiered approach to categorizing all BES Cyber Systems according to impact.

There was a comment that the standards use the term "Transmission stations or substations," and the commenter proposed some other terms such as "switchyards." The SDT points out that a brief clarifying paragraph is included in the Guidelines and Technical Basis explaining the use of these terms in the section on Transmission criteria: "*The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain*

autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist." The SDT also made minor editorial changes when using this term for more consistency.

There was a comment that the paragraph in the Background section that deals with the 300 MW UFLS threshold should be moved to the Guidelines and Technical Basis section. The SDT points out that section 4 is a common section that is in all the standards and believes that the explanation of the 300 MW threshold used in the common section 4 should be included in the common part of the Background section to carry it into all the CIP standards in this series.

One commenter provided general feedback on the approach taken for CIP-002-5. The commenter cited concerns on the Facilities-based approach to evaluating the impact of BES Cyber Systems. The SDT had extensive discussions in the last several years on the merits of both the systems-based and facilities-based approaches. The SDT points out to the commenter that entities are free to use any method to arrive at the identified and categorized BES Cyber Systems. Regarding the evaluation of the impact based on the function of the assets, a fundamental concept in risk management frameworks, including the National Institute of Standards and Technology (NIST) Risk Management Framework, is that the evaluation of the risk for systems must be related to the mission of the organization, in this case, the reliability of the BES. The entity also commented on the lower level of protection for low impact BES Cyber Systems. This is consistent with tailoring the level of protection according to the risk (in this case, the impact) and optimizing available protection resources for the systems that most need the protection according to their impact on the mission of the organization. The commenter also commented on the consideration of "interconnectedness". The SDT has taken the approach of considering connectivity in the development and application of Requirements.

There was a comment made that the section on BES reliability operating services in the Guidelines and Technical Basis section should be removed as it contains many subjective areas. The SDT has gone through several iterations of including these in the standards or as guidance and has resolved to providing guidance on functions for applicable functional entities based on the functional model. The section has been well-received with comments requesting the included enhancements in the past drafts.

A recommendation was made that the undefined term "adversely impact" should be replaced with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. The SDT disagrees, because where the SDT has used the term Adverse Reliability Impact, it has used it precisely for the meaning defined in the NERC Glossary. It is not appropriate to use the NERC Glossary term when it is not the intent of

the SDT to use the meaning of the defined term. The NERC Glossary term is very specific to a level of impact on the reliability of the BES. This is not always the appropriate level or meaning in all cases where the term "adversely impact" is used.

One commenter noted that the diagram at the end of the Guidelines and Technical Basis section is confusing. In response, the SDT notes the flowchart is an actual use case provided by an observer and may not be applicable in all environments. It is meant to provide one approach used by an entity.

Requirement R1

There were several commenters that noted there was inconsistency in the words used in Requirement R1 and Attachment 1, criterion 3.4 of section 3 (Low Impact), regarding restoration, with terms used in EOP-005-2 and with terms used elsewhere in the standard. The SDT has made changes to these sections to be consistent with the terms used in EOP-005-2: Blackstart Resources and Cranking Path and initial switching Requirements.

One commenter requested that additional reference to the specific standards be included where the term "...is subject to one or more Requirements in a NERC or Regional Reliability Standard" is used. The commenter furthermore stated that this term is not specifically used in Requirement R1 or the Requirement Parts. However, it is used in section 4 to qualify UVLS/UFLS, Special Protection Systems and Protection Systems owned by DPs that are subject to these CIP standards. In response, the SDT notes the intent is to include only those assets for DPs that are covered by a NERC Reliability Standard, which would be those, by implication, that are related to the reliable operation of the BES. References to other standards within a standard are not recommended practice in NERC standards drafting.

There was a comment that the last sentence in the opening paragraph for Requirement R1 in the Guidelines and Technical Basis section for Requirement R1 is confusing. The SDT has clarified and simplified the sentence.

One commenter stated that the use of the term "considers" in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that "consider" does not mandate a required subsequent action. The commenter proposes that the Requirement should be restated as "For each asset type enumerated below, each Responsible Entity shall: . . ." In using the term "considers", the SDT recognized that all entities do not own all the types of assets listed. The proposed language assumes that all entities own all of the types of assets listed. In providing this consideration, the SDT seeks to avoid situations where entities end up having null lists for each one of the type of asset that it does not own.

The same commenter stated that the assertion in Requirement Part 1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this Requirement not auditable for accuracy or completeness; and that to demonstrate that all high and medium impact BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impact BES Cyber Systems. The commenter further stated that the entity must be prepared to demonstrate the minimal Requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. The SDT has considered the considerable increase in the scope of cyber systems included in this version and has taken the approach that those Requirements that apply to the anticipated large number of low impact field systems should be focused on program components that provide the corresponding level of protection, rather than a disproportionate effort in managing compliance for these systems.

One commenter suggested the removal of Requirement Part 1.3 and the low impact category in Attachment 1. The SDT has taken the approach that all BES Cyber Systems should be subject to some level of protection. The SDT has provided an approach to allow the specification of the commensurate level of protection for low impact cyber systems while providing a framework that would minimize entities' compliance burden for the large number of low impact cyber systems that it anticipates.

One commenter recommended that the six asset categories included as part of Requirement R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. The inclusion of the asset types in Requirement R1 is a direct result of comments from a large number of stakeholders on draft 2 to provide some reference to asset types required to be considered in Versions 1 through 3. The SDT has made modifications to improve overall consistency within the standard.

Another commenter noted that, in Requirement Part 1.3, the intent is to provide protection at BES Facilities that do not meet Attachment 1, criteria 1.1 through 2.13. The commenter added that the wording is technically flawed and conflicts with the definitions of BES Cyber Assets and BES Cyber Systems. The commenter continued to add that, by definition, to qualify as a BES Cyber Asset and System the asset must have a 15 minute impact on reliability of the BES and that a low impact facility cannot have such an impact to the BES. The SDT points out that while the definition of the BES Cyber System and BES Cyber Asset assumes impact on the function of the Facilities, systems and equipment (asset), an asset in the low impact does not assume that it has no impact on real-time operation of the BES. The 15 minute stipulation in the definition of BES Cyber Asset describes an impact on the function performed by the low impact asset for the BES.

One question arose which asked how an auditor is to verify identification of all BES Cyber Systems that are applicable to Requirements Parts 1.1 and 1.2. There are current Requirements to identify Critical Cyber Assets in Versions 1 through 4. The SDT expects that auditors will continue to use similar methodologies used to verify compliance to such Requirements.

One commenter stated that its interpretation of Requirement R1 meant that each qualified cyber asset must be marked. This is not the intent, and the SDT does not believe that the language in Requirement R1 is specifying any such marking for cyber assets at each asset. The clause "at each asset" is purposely included in close proximity to "BES Cyber Systems," which is the phrase that "at each asset" is intended to qualify, not the word "identify". Certainly, the expectation is that the identification of the BES Cyber System would include information in some fashion about which asset it is "at". The proposed language "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," does not meet the intent of the Requirement, since it must be clear that the identification must have enough information to identify the BES Cyber System, including the information on what asset it is located at.

Requirement R2

Many commenters noted that alternative, clearer language for Requirement Part 2.1 would ensure that there is no implied Requirement for updates outside of the annual Requirement review. The SDT believes the 15 month review is sufficient for categorization of BES Cyber Systems, and it has modified the language to provide additional clarity.

Attachment 1

There was a proposal that the language should be modified to specify that the applicable functional obligations referenced within criteria 1.1 through 1.4, 2.11, and 2.12 apply to only those real time tasks identified in the Functional Model. The SDT points out that the applicability of the Requirements is to BES Cyber Systems, and that the definition of BES Cyber Assets (and by reference, BES Cyber Systems) only includes those that impact real-time operation. The functional model does not define the tasks of the functional entity in terms of real-time or non-real-time, but the term real-time is used rather to describe its relationship with other functional entities.

Many commenters reiterated their comment on the rationale for categorization as high impact those Control Centers that control at least one of the medium impact facilities. The SDT responds that the localized impact of a facility at a single location is different and less impactful than the impact of a Control Center that controls one such facility and other facilities in the wide area.

There was one comment that stated Attachment 1 does not specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. The SDT clarifies that these systems used to perform functions that are not impactful to real-time operation of the BES, as such would not be defined as BES Cyber Systems, unless these systems are also performing functions impactful to the real-time operation of the BES. They would be included in scope in the initial scoping of supporting the functional obligations of the relevant functional entity, but systems strictly performing these functions in the absence of other functions impactful to real-time operation would fall out of scope.

There was a comment that the first bullet under the overall heading of the Guidelines and Technical Basis section for Attachment 1 makes several references to the term "BES Asset." The SDT has corrected the inappropriate capitalization of BES asset and uses the term BES asset as referenced in Requirement R1 of CIP-002-5.

One commenter expressed concerns that restoration facilities were categorized as low impact facilities. This issue was raised in comments received in previous drafts and the SDT has discussed this at length, reaching out to other NERC technical committees. After consideration of the overall risks to the availability of adequate restoration resources, the SDT's resolution was to categorize restoration facilities as low impact, as explained under the Guidelines and Technical Basis section of CIP-002-5, on pages 30 and 31.

Many criteria in Attachment 1 relate to Interconnection Reliability Operating Limits (IROLs). One commenter wrote that this may be a problem in the WECC area where the RCs have not yet defined IROLs. Consultation with WECC indicated that WECC is in the process of defining IROLs and that IROLs will be defined well within the implementation timeline of these standards.

Another commenter stated that since the term "associated data centers" has been removed from Attachment 1 and that it should be removed from the Guidelines and Technical Basis section. The term has been moved to the definition of the Control Center and an additional clarification has been included where it is referenced in the Guidelines and Technical Basis section.

Criterion 1.2

One commenter noted that the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing Authority (BA) has not only upon its own service area but also

upon the rest of North American BA, Reliability Coordinator (RC), and TOP registered entities with which it is directly or indirectly connected via the ICCP communication networks. The SDT carefully considered discussions from stakeholders and reviewed data on the distribution of BAs that would be affected. The SDT concluded that the threshold would include the majority of BAs with significant impact.

Criterion 1.4

Many commenters noted that this criterion would require that a 1500 MW Generator Operator (GOP) Control Center take on a High impact rating, while the rest of the Facility is medium impact. The commenter added that even if the criterion is intended to apply to multiple locations, the aggregated generation should be 3000 MW or greater - consistent with the risk level assigned to a BA Control Center. The SDT points out that a control room for a single generating plant at a single location does not meet the definition of a Control Center. The criterion has not defined a specific numeric bright line for a generation Control Center. For example, a generation Control Center could control three 1200 MW generation Facilities, for a total of 3600 MW, at more than one location, and still be qualified for a medium impact generation Control Center if none of these meet criteria 2.1, 2.3, 2.6 or 2.9. It is true that if one of the generation Facilities the Control Center controls meets criterion 2.1 for 1500 MW, it would be categorized as a high impact asset.

Criterion 2.1

One commenter requested clarification on the relationship between a single plant location and a single Interconnection used in the defined term meaning. In making these qualifications, the SDT considered scenarios where sets of units within a single plant location may service multiple Interconnections, as pointed out by the commenter. In these cases, the SDT wanted to ensure that the impact considered is consistent with the bright line defined in this criterion, which was based on numbers reviewed for each Interconnection. The same entity inquired about “multiple generators with different interconnection facilities which connect to different parts of the same substation.” It is not clear whether the commenter is using the general term interconnection (meaning connection to the Transmission System) or in the meaning of the defined term.

One commenter felt that the use of the word “by” in the first sentence of this criterion does not make sense and should be reworded. The use of the word provides an entity with the capability of evaluating groups of units when a single plant location may be servicing multiple Interconnections and is logically partitioned into more than one generation output. There are further qualifications which may provide additional grouping criteria, such as common cyber systems.

One commenter suggested that the 15 minute stipulation should be extended to 30 minutes to be consistent with some criteria in reliability standards. Some standards have used 15 minutes, which the SDT has used as its criterion. The commenter seems to suggest that the 15 minutes is "tighter" than 30 minutes. Extending the interval to 30 minutes would in fact reign in more cyber systems rather than reduce the number of cyber systems (by extending the criterion for real-time, more cyber systems are likely to meet this criterion than 15 minutes).

One commenter requested clarification on the term "commissioned generation." The term is used to specify generation resources that have been commissioned for operation and is intended to exclude generation that has not been commissioned for operation (such as mothballed generation, generation shut down for maintenance, or new generation that has not been commissioned for operation yet).

Criterion 2.3

There were many comments that the term "planning horizon of one year or more" is unclear and could be misinterpreted. The SDT has added guidance on this to make it clear that the planning horizon of one year or more means that the plan covers a reliability planning span of one year or more and that it does not necessarily mean that the operating day is over one year. The intent is to exclude generation required to operate or keep on operating to temporarily avoid reliability impacts.

There were many comments on the guidance relating to the role of the Regional Entity (RE)/ Regional Reliability Organization (RRO) and noted that the RE/RRO is not required to perform coordination of the actions resulting from planning studies. The commenter also noted that the term RRO is no longer the appropriate term. The necessary changes have been made.

One commenter asked whether the term "generation Facility" in this criterion is designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1. The SDT intended to include in this criterion all generation Facilities required to meet the designation: these can be a single unit, a set of units or all the units in the plant.

One commenter noted that the Guideline and Technical Basis section omitted the TP as one of the possible entities that could designate the generation Facilities. The SDT notes this has been corrected.

A commenter asked whether the phrase, “such as due to a Category C3 contingency” was intended to provide guidance to what faults to run and whether the term “Adverse Reliability Impact” which is used in Attachment 1, meant to be the criteria for all types of contingencies. The phrase “such as due to a category C3 contingency” is intended to provide an example of the type of condition that could lead a Planning Coordinator (PC) or Transmission Planner to designate “must run” generation Facilities. The term “Adverse Reliability Impact” is used here to qualify the reason the PC or TP would designate such generation Facilities. In response, the SDT notes it is intended to distinguish from designations made for power market management reasons.

One entity commented that the guidance provided in this section in the Guidelines and Technical Basis section referenced “Reliability Must Runs (RMRs)” and discussed the differences between market RMRs and what this criterion intended. The SDT points out that this is the reason it has avoided using the term “reliability must run” in the Requirement itself. However, this term has been used interchangeably in both contexts for lack of a better term, and that the meaning of the term and the reason for having these units differ depending on the context. The SDT has included an extended discussion of the underlying reason for the criterion in the Guidelines and Technical Basis, focusing on the long term remediation for BES deficiencies to avoid Adverse Reliability Impact. The SDT also made additional changes to the guidance to clarify the role of the RE in coordination and contracts.

There was a comment that the criterion is based on studies from functional entities that do not have applicability under this standard and on notifications from these entities. The SDT notes that these activities are implemented today and that there are TPL standards that require these functional entities to perform these studies. The standard also requires these planning entities to provide an action plan for remediation of identified deficiencies.

Criterion 2.4

In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. One commenter noted that exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. The commenter further noted that specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. The applicability, which is section 4, stipulates applicability to BES Facilities for entities other than DPs. If the facility meets the qualification for designation as a non-BES facility under the definition of the Bulk Electric System, then it is not in scope for application of these CIP standards.

Criterion 2.5

One commenter noted that the 200kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200kV. The commenter noted the BES is defined as 100kV and above and the criterion needs to consider all of the BES in some manner. The SDT has not excluded any BES Transmission Facility in its applicability, but believes that not all BES Transmission Facilities should be protected at the medium impact level. The categorization is one that is based on impact, and the SDT believes that the inclusion of ALL BES Transmission Facilities at a single impact category is unjustified and defeats the concept of tiered levels of protection based on impact.

One commenter stated that, as currently defined, the values in the table force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. The commenter recommends the values be revised as follows: Voltage Value of a Line 200kV - 399kV - Weight Value per Line - 800; Voltage Value of a line 400kV to 499kV - Weight Value per Line - 1300. The SDT based the values in the table on values published in an engineering report, has reviewed comments from previous drafts, and believes that it has a technical basis, as described in the Guidelines and Technical Basis section, for using these values.

A commenter provided an extensive discussion of the concerns on the application of this criterion for Direct Current (DC) Facilities. The commenter argued that in the case of DC Facilities, the impact is better assessed in a wide area perspective rather than as a localized way as specified in this criterion. The commenter further commented that such studies could be conducted to provide an impact based on MW rather than the approach used in 2.5 in the case of DC Facilities. The SDT has not considered this approach for DC Facilities and any criterion that is based on a "study" (that is not currently required by any reliability standard) to determine the impact of these DC Facilities would be contrary to the bright line approach.

One commenter requested that diagrams be provided to illustrate the bullets in the Guidelines and Technical Basis. The SDT discussed providing diagrams to illustrate the bullets, but resolved that there are many configurations that can provide these illustrations and that these would raise additional questions for entities that would not be familiar with specific configurations. Entities should use their specific configuration to apply these concepts.

One commenter requested many clarifications. These are listed below with their responses:

1. Is/how is a DC line counted?
   A DC line is counted at the operating voltage for the purpose of application of criterion 2.5.

2. If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line?
   If the transformer in at the site of a Transmission station or substation, it is considered as part of the Facilities of that station or substation and lines incoming and outgoing of the station or substation are considered in the application of this criterion. If the transformer is in a dedicated station, each of the stations (including the transformer station) will consider incoming and outgoing lines of the station or substation in the application of the criterion.

3. From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub?
   These examples are all considered as a radial connection to a single generation facility.

4. From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities.
   The clause "In these cases" is qualified further by "of these transformers being within the "fence" of the substation or station": this is referring to what is considered a single facility.

5. From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service?"
   Assuming that the tap is at the station or substation, these would be considered connections to one other substation, but both outgoing lines would be counted for the purpose of aggregate weighting. If the tap is not at the station or substation, there is not enough information to definitively make a determination without evaluating the specific facts and circumstances.

One commenter inquired during the comment period on whether the connections to other stations or substations that are considered are only those that are operating at voltage levels between 200kV and 499kV. The SDT reviewed previous drafts and clarified the criterion to ensure that the qualification of voltage levels of 200kV and higher for these connections is more explicitly stated rather than implied.

Criterion 2.6

One comment was on the obligation for the RC with respect to IROLs. RCs are required to provide to its TOPs in its RC footprint the SOLs under FAC-014-2, Requirement R5.1. In particular, it requires the RC to provide specific information related to IROLs in the sub-Requirements of 5.1. The particular agreements between RCs, TOs and TOPs to enable the proper management of IROLs in compliance with the NERC Reliability Standards are beyond the purview of the guidance. The SDT points out that the delegation of functional obligations must be considered in these Requirements.

Criterion 2.8

A commenter noted correctly that Transmission Facilities under 2.8 that do not affect Transmission, in aggregate, for generation that is less than 1500 MW do not qualify under this criterion, even if the generation facility (plant) contain cyber systems that qualify under 2.1., (provided they do not qualify under other criteria).

Another commenter noted that, in the case where the generation is not owned by the TO/TOP would be at the mercy of the Generation Owner's (GOs) application of the standard even if the TO's facilities would not otherwise be in scope. The commenter is correct in that the TOs Facilities providing the connection would be deemed to be a medium impact. This is consistent with the impact of these Transmission Facilities on the BES.

Criterion 2.9

One commenter requested clarification on what an automated switching system is. Automated switching systems refer to systems implemented in software that perform the same automated protection functions as Special Protection Systems or Remedial Action Schemes.

Criterion 2.10

One commenter stated that the guidance document specifies that the SDT "chose the term 'each' to represent that the criterion applied to a discrete System or Facility". The commenter's interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level and that an individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. The commenter's interpretation is partially correct in that individual independent relays that are part of a UFLS system that sheds 300 MW or more in the program Requirements, but do not shed the required load by a common control system, (e.g., they individually trigger independently, even if they are configured to trigger based on the same sensed conditions) do not qualify. However, if the individual relays are all triggered automatically by a common control system that determines

that conditions warrant the action (such as a control panel that triggers a system of relays in a substation), then they are part of a load shedding system that can automatically shed more than 300 MW and therefore qualifies. The commenter's assertion that a single relay that sheds 300 MW or more does qualify is correct.

The same commenter noted the statement on ERCOT's LaaR demand/response program is not considered as qualifying under this criterion and requested more general guidance in the Guidelines and Technical Basis section for this criterion that talks to these types of programs. The SDT has included a more general statement in this section.

Criterion 2.11

There was a comment that the Guidelines and Technical Basis section on this criterion incorrectly referenced a 300 MW threshold. The SDT has made the necessary correction.

Criterion 2.12

Many comments related to the portion of criterion 2.12 of Attachment 1 that is applicable to TOP Control Centers. Commenters stated that criterion 2.12 of Attachment 1 included all TOP Control Centers, not already categorized in the high impact category, as medium impact and that many smaller TOP entities' Control Centers should be categorized as low impact in the same manner that criteria were defined for generation and balancing authority Control Centers. Many commenters proposed alternate proposals for a threshold that could provide such a criterion to be used as a candidate for categorization as low impact, such as voltage levels lower than 200 KV or using throughput indicators similar to those used in the case of transmission substations in criterion 2.5. Others provided proposals to restructure the thresholds for all three impact levels for TOP Control Centers. One commenter also proposed an exclusion clause in criterion 2.12 that would be based on engineering analysis that demonstrated minimal impact to the BES. In response, the SDT did not find any such study that would be required by an existing NERC Reliability Standard.

As part of a consolidated response to more than one entity that provided comments on draft 2's CIP-002-5, Attachment 1, criterion 2.11 (which maps to criterion 2.12 in draft 3 and draft 4), the drafting team carefully considered comments to include a threshold for TOP Control Centers, but, to reiterate previous considerations and response to the comments related to that criterion (on page 35 of consideration of comments form A), such a threshold is not supported in consideration of the functions provided by those Control Centers. The largest concentration of cyber traffic is to and from Control Centers, and loss, compromise, or misuse of cyber systems at control centers constitutes a high risk to reliability. Furthermore, criterion 2.12 applies to "Control Centers" used to perform the functional obligations of TOPs, so it is only applicable to the extent the Control Center meets the criteria of the proposed definition.

While there is clear guidance in the NERC Reliability Standards that the SDT could use to determine bright lines for generation in the wide area (such as contingency reserve Requirements), the SDT did not find any in the Transmission area to support thresholds for TOP Control Centers. The source for transmission substation bright lines, based on throughput in a Transmission station or substation according to voltage level, provided easily measureable thresholds because of their localized nature: for a given single location, the application of the threshold criteria can be easily determined. There was no bright line that the SDT could find applicable and justifiable in a wide area situation for TOP Control Centers that control many interconnected Transmission Facilities in many locations. The SDT could not find any technical guidance, either in NERC technical studies, or in existing NERC Reliability Standards Requirements, on how the loss of interconnected Transmission Facilities could be used as a basis for establishing thresholds for TOP Control Center impact. The TOPs span of control is not limited to just Transmission lines, but to a large number of diverse Transmission Facilities that relate to the reliable operation of the BES. This complexity, together with the interrelated impact from the large number of diverse Functional Entity types that impact TOP functional obligations, make it very difficult to define a justifiable threshold that can be rationalized considering all the scenarios that could impact real-time operation for a TOP Control Center.

As stated in the guidance for CIP-002-5, the reasoning and purpose for the 1500 MW threshold for generation is different:

> "By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that BES Cyber Systems with common mode vulnerabilities that could result in the loss of 1500 MW or more of generation at a single plant for a unit or group of units are adequately protected."
>
> The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used."

Furthermore, the SDT has an obligation to be responsive to FERC Order No. 706, which was issued after a notice of proposed rulemaking, and several points from that order were reiterated in subsequent FERC Order No. 761. The SDT has discussed this issue very significantly in several face-to-face SDT meetings. In addition to the technical reasons and differences explained above, the SDT anticipates that any threshold for TOP Control Centers will likely be met with a directive countering such threshold upon filing for approval of these standards.

The SDT based its approach in the development of this criterion in consideration of the following comments and Directive from FERC Order No. 706 approving CIP Cyber Security Standards Version 1 and FERC Order No. 761 approving CIP Cyber Security Standards Version 4.

In its Order No. 706, Para 280, FERC supports the reasoning for its subsequent Directive in paragraph 282 with the following comment:

> "...it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset…"

The SDT points out that Medium and High Impact under Version 5 translate closely to "Critical Asset" under previous versions. The Directive in FERC Order No. 706, Para 282 further states:

> "Therefore, consistent with the discussion above, the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets."

As explained earlier, the SDT's consideration of misuse of TOP Control Centers and the role they provide, pursuant to this Directive, do not support an exclusionary threshold from medium impact in CIP-002-5, Attachment 1.

In its Order 761 approving NERC CIP Cyber Security Standards Version 4, FERC commented in paragraph 21 that:

> "...Version 4 will offer an increase in the overall protection for bulk electric system components that clearly require protection, including control centers"

In the same Order 761, Para 57, FERC further commented with the following:

> "However, we continue to expect comprehensive protection of all control centers and control systems as NERC works to comply with the Requirements of Order No. 706."

Again, in the case of Generation and BA Control Centers, the SDT used the 1500 MW threshold for consistency with the rationale used for generation bright lines. As stated, no such source can be used for wide-area transmission in the non-CIP reliability standards or other published source.

Therefore, the SDT opted to keep criterion 2.12 as it applies to TOP Control Centers (i) to ensure that all TOP Control Centers are adequately protected, in the absence of technically justifiable thresholds for lower impact TOP Control Centers, (ii) because of the critical nature of their real-time reliability functions for the interconnected Transmission systems they monitor and control, and (iii) in consideration of FERC comments and Directives expressed in Order No. 706 and reiterated in Order No. 761.

Criterion 2.13

One commenter believes that the 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of BAs from meaningful participation in protecting the BES from cyber-attack and that establishing criteria effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both FERC Order No. 706 and FERC Order No. 761. The SDT considered the MW distribution of BAs and determined that the 1500 MW is consistent with generation thresholds established (and approved by FERC in Version 4) in other criteria and is appropriate in including a significant number of BAs at the medium impact category. The SDT points out low impact cyber systems are still subject to protection Requirements.

Criterion 3.1

There was a comment that criterion 3.1 should specifically state that only Generation and BA Control Centers are included. While combination of the criteria for Control Centers currently results in only Generation and BA Control Centers, this criterion is intended to catch all Control Centers that have not already met a previous criterion in section 1 and 2 (high and medium impact). The current language conveys this intent.

Criterion 3.4

One commenter stated that the use of the terms “critical” and “initial system restoration” in criterion 3.4 is problematic. The commenter noted that initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The SDT has made modifications to the criterion that uses language consistent to EOP-005-2 and defined terms.

The commenter also noted that the Low Impact Rating criteria needs to include automatic Load shed systems that do not shed sufficient Load to meet criterion 2.10. All Load shedding systems that are part of the BES are included automatically as stated in the Applicability section (section 4). For DPs, Load shedding systems that meet the qualifications in section 4 are included and are all included as medium impact.

CIP-003-5

CIP Senior Manager

A commenter expressed concern on the designation of the CIP Senior Manager by a "high level official" and whether that official could be the same person as the CIP Senior Manager. The SDT notes that the language regarding "high level official" is but one example in the measure. An entity is free to determine the best way to designate a CIP Senior Manager for its unique circumstance. This could be by high level official, by committee, through authorization from a board of directors, or from any number of other options.

The SDT received a comment that there was a concern that by only requiring the identification of the CIP Senior Manager by name that the Requirement was not auditable in instances where multiple individuals have the same name at the same company. The SDT appreciates that this is a very real scenario. However, the SDT believes that this is specifically the style of auditing that it sees is incompatible with the objectives it is setting out to achieve. The SDT believes that real cyber security program leadership transcends the name on the document. Audits, instead of verifying a name on a page, should instead validate the Requirement objective that the individual identified as the CIP Senior Manager is in fact leading and managing the implementation and continuous adherence to the CIP standards.

One comment indicated that "The CIP Senior Manager relies on both the definition in the CIP Glossary and the "Responsible Entity" verbiage in every standard in section 4." The SDT does not agree. The definition of a CIP Senior Manager stands alone. However, the Requirement itself is for the Responsible Entity (the entity obligated to comply with the standard) to identify a CIP Senior Manager.

Policy Requirements

One commenter expressed concern that the SDT was too prescriptive in its language around electronic access controls in the low impact policy. The SDT does not believe this to be the case. On the contrary, the SDT has some concern that it may have left the policy up for too much interpretation. However, the SDT believed that the entity is in the best place to determine the appropriate access controls for its given situation, while still implementing an ESP of some form.

Numerous commenters expressed confusion over the applicability of the policy Requirements. The SDT considered many approaches to this issue and believes that the applicability of these requirements is clear as drafted. Requirement R1 applies to high and medium BES Cyber Systems and states as much explicitly in the Requirement. The intent of

Requirement R2 is to apply to those assets that contain low impact BES Cyber Systems and not to the BES Cyber Systems themselves. This effectively allows the entity to track implementation of the policy at a higher level of abstraction (per asset rather than per BES Cyber System), and the SDT believes this will substantially reduce the burden of evidence required by the low impact policy. The reference to CIP-002-5 is to further clarify the intended reference to asset rather than BES Cyber System. The language following the numbered list specifying that "an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required" is part of the Requirement language of Requirement R2 and should be interpreted as such. This language was explicitly included to give the industry the assurance that this Requirement would be audited (sampled) at the asset (substation, generation plant, etc.) level and not the individual Cyber Asset level. The SDT also believes that entities will be able to implement internal controls to ensure the implementation of the cyber security policy at its low impact assets. The SDT does not believe that there is any double jeopardy between Requirements R1 and R2.

One commenter suggested that the SDT modify the Requirement language for the cyber security policies to clarify that multiple policy documents could "collectively" address the topics in the Requirements. The SDT agrees and has updated the standard to reflect this change.

The SDT received comments that Requirements R1 and R2 require annual review of the policy, but never explicitly require the policy to receive updates as a result of that review. The SDT believes this is implicit in the Requirement, and updates would occur as part of an entity's ongoing compliance with the Requirement.

Requirement R2

One commenter questioned the necessity of Requirement Part 2.4 considering that entities are not required to monitor for incidents to their low impact BES Cyber Systems. The SDT appreciates this concern. This element was specifically included because the SDT strongly believes that incident response is a key component of a resilient system. Even though an entity may not be constantly monitoring for a Cyber Security Incident at its low impact BES Cyber Systems, the SDT expects that should an incident be discovered, a plan should be in place for rapid execution.

Requirement R4

The SDT received comments requesting that language be added into the Requirement clarifying that the delegation authority may itself be delegated. The SDT considered adding language to the standard to clarify this, however, the SDT believed that the Requirement was clear as is and that there was no language that prevented this delegation. The SDT included the discussion on this topic in the Guidelines and Technical Basis section specifically to clarify this issue.

One commenter pointed out that Requirement R4 as written requires that the delegations from the CIP Senior Manager be updated within 30 days of the initial delegation. The SDT agrees this is confusing and has struck this language from the Requirement.

The SDT received questions on why it included the IAC language on the Requirement to delegate authority from the CIP Senior Manager. The SDT specifically included the IAC language because it believes that in a very large organization, it is likely that changes in personnel without adequate update of delegation documentation could result in very minor deficiencies that have little or no impact on the reliability of the BES. These are precisely the types of administrative violations that the SDT is attempting to eliminate from the CIP standards. The SDT believes that, given this is all a single Requirement, the documentation required in the third sentence of Requirement R4 is part of the overall process specified in the first sentence of the Requirement; consequently, the IAC language applies to all parts of Requirement R4.

CIP-004-5

General

One commenter believes that the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs, RCs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. Entities are required to demonstrate compliance with the Requirements for the entire audit period for all NERC Reliability Standards, regardless of evidence retention Requirements.

One commenter noted that within each Background section (section 5) under the heading "Applicable Systems Columns in Tables" is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. The SDT confirms that it intended that phrase to be consistent wherever that applicability term was used, and the SDT has modified the background to clarify that intent.

There was a comment that within CIP-004-5, the definition of EACMS appeared inconsistent with the definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards", and that it could result in misidentification, misapplication or inconsistent application of standards. The SDT has modified the background section with respect to EACMS to provide clarification that these are examples only that support the definition.

Requirement R1

A few commenters requested that Requirement R1 include the IAC language. In response, since the Requirement may be performed at any time during the quarter, the addition of the IAC language would not be appropriate.

One commenter requested clarification on the types of materials to be provided for security awareness on a quarterly basis. The Requirement is to provide an ongoing reinforcement that cannot be provided by an annual training Requirement. The SDT has written the Requirement to allow for flexibility in implementation by the entity. The measure provides some examples of how the entity may meet this Requirement.

A few commenters considered Requirement R1 to be administrative in nature and suitable for elimination pursuant to the SAR Paragraph 81 project. While this Requirement is partly administrative, it does provide the benefit of the entity being able to timely address and make staff aware of emerging threats and vulnerabilities. This awareness can improve security for the entity.

One commenter requested that Requirement Part 1.1 be modified as, “cyber security practices and/or physical security practices.” The SDT clarified that the Requirement part applies to cyber security, which may include awareness on associated physical security.

Requirement R2

One commenter recommended that the training content Requirement Part 2.1 be moved to the measures. The SDT considered the training topics listed to be worthy of being listed as a Requirement for a minimal core competency in security practices. Entities are encouraged to add more topics as relevant to their needs.

One commenter recommended that Requirement Part 2.2 be modified to address newly registered entities. In response, the compliance dates for newly registered entities are addressed in the supplementary implementation plan provided with the Version 5 standards.

One commenter considers it is a security risk to address some of the concepts listed in Requirement Parts 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided.

Several commenters requested clarification on the necessary training for personnel based on individual roles, functions, or responsibilities, including changes to roles, functions, or responsibilities. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a security training program that fits their needs. The Requirement does not preclude an entity from using a single or multiple training courses with differing depth in the training provided. How the training program is implemented is at the discretion of the entity.

One commenter requested that CIP Exceptional Circumstances be removed from Requirement Part 2.2, as this applies to numerous parts and is stated at the policy level. The SDT believes that, as written, the Requirement provides necessary guidance related to the Requirement without introducing the need to rely on or link to other Requirements.

One commenter requested clarification on whether the training required by Requirement R2 extends to contractors and vendor support staff. The SDT notes that, as written, the Requirement is clear that training is to be provided to anyone having authorized electronic access and authorized unescorted physical access.

One commenter requested that Requirement Part 2.1.9 be removed. The SDT considers the training topic relevant to address the vulnerabilities of internetworked systems and to address the risks of systems that are integrated and reliant upon data from other sources to perform necessary tasks (interoperability).

Requirement R3

Several commenters noted concerns regarding Requirement R3 where employee history is not available, including the identity verification necessary to perform the criminal history check, and how to comply with these instances. The Requirement provides for this, "If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed."

One commenter requested that the timeline for personnel risk assessments pursuant to Requirement R3 be modified to 10 years to align with other governmental standards and practices. The SDT is not clear if the commenter means performed every 10 years or reviewing the prior 10 years for criminal history. The SDT has kept the timing Requirement of the existing standards as approved by FERC Order No. 706.

Many commenters requested clarification for Requirement R3 that ongoing identity verification is not required. The SDT has noted in guidance and the implementation plan that identity verification is required only initially. However, the Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets their needs to confirm identity. For some, this may include performing subsequent identity verification or it could include confirmation of previous verifications.

One commenter noted grammar concerns with the Requirement R3 table parts. The SDT believes that the overarching Requirement provides the necessary context and clarity for the table.

One commenter stated Requirement Part 3.3 unclear as to whether the evaluation process includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. The SDT has modified the Requirement to make this clearer.

Two commenters considered Requirement Part 3.4 unclear as to whether the entity is to perform the evaluation or permits the contractor or service vendor to perform the evaluation using its own criteria with an assertion to the entity of compliance and acceptability. The SDT believes that, as written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits their needs. The entity is responsible for ensuring that the obligations of the Requirement are met by their contractors and service vendors.

One commenter requested that the table parts for Requirement R3 be modified to require that a personnel risk assessment must be complete before granting access. The overarching Requirement R3 states that a personnel risk assessment is required in order to obtain access.

One commenter requested that Requirement Parts 3.5 and 3.6 include a clause that it is subject to applicable law and collective bargaining unit agreements. This concern is addressed in the guidance provided for Requirement R3. As written, the Requirement is flexible to allow the entity to design and implement a personnel risk assessment program that fits its needs.

Several commenters requested clarification on whose identity must be verified. As written, the Requirement is clear that personnel risk assessment is to be performed for anyone having authorized electronic access and authorized unescorted physical access. This is further defined in Requirement Part 3.4.

One commenter recommended consolidation of Requirement Parts 3.3 and 3.4 into Requirement Part 3.2. As written, the Requirement defines each individual element to be performed and that these are each elements contained within the program specified by Requirement R3.

One commenter considered Requirement Part 3.3 redundant of Requirement Part 3.2. Requirement Part 3.2 is the performance of the criminal history records check. Requirement Part 3.3 is the evaluation of the records collected under Requirement Part 3.2.

Requirement R4

A few commenters noted concerns regarding the efficacy of Requirement Part 4.2. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the

records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

One commenter recommended that Requirement Part 4.2 be removed and provide it as an example of an internal control that the Compliance Enforcement Authority (CEA) would expect to see. The SDT considers this Requirement as a key element for security. The intent of the Requirement is to review the accounts residing on the systems with the records of what accounts are supposed to be on the systems. This helps to provide an assurance that accounts have not been added through malicious code and that provisioning processes are functioning properly.

Several commenters requested clarity in Requirement Part 4.3 related to which accounts and types are subject to an annual review. Individual user accounts, user account groups or user roles are required to be reviewed on an annual basis. User account groups or user roles are to be reviewed where these are used to for role-based management of access permissions. While review of other account types (i.e.: default account) is a good security practice, it is not a Requirement under the CIP Version 5 standards.

One commenter requested clarification of Requirement R4 regarding the word "verify" and how an entity is expected to provide evidence of access control. The Requirements mandate that access is limited to only those requiring said access. It is the responsibility of the entity to determine how they can demonstrate this limitation through the use of technical or procedural controls. The SDT believes the Requirements are written to allow flexibility in implementation to allow the entity to develop a program that meets its needs. The use of access controls lists, key control processes, and log books should be considered as options.

There was a comment that the phrase "based on need, as determined by the Responsible Entity" within Requirement Part 4.1 does not add anything meaningful to the standard. The SDT added the language based on industry comment concerns to help clarify that the appropriateness is determined by the entity and not by the CEA.

One commenter stated that the concept of role-based privilege management has not been established adequately in the Requirement. The SDT believes that Requirement Part 4.1 is written with sufficient flexibility to allow the entity to implement access control processes that meet their needs. The Requirement does not preclude the use of role-based privilege management. Requirement Part 4.3 has been modified to address this concern.

One commenter requested clarity on the measures for Requirement Part 4.2. The measures are examples of how the Requirement may be met. They are not an all-inclusive list of possibilities. It would not be feasible to list all options available.

One commenter noted concerns regarding Requirement Part 4.3 related to the level of access permission review to be performed. The detailed access privileges are to be reviewed to determine if they are appropriate. This can include review of access to file systems. As noted in the guidance, "The privilege review at least once every 15 calendar months is more detailed…"

Several commenters requested clarification regarding the verification of access to information storage locations pursuant to Requirement Part 4.4. As noted in Requirement Part 4.1, there are three distinct types of access noted; (1) Electronic access, (2) Unescorted physical access into a Physical Security Perimeter (PSP), and (3) Access to designated storage locations, whether physical or electronic, for BES Cyber System Information. The intent of Requirement Part 4.4 is the review of access to BES Cyber System Information only.

One commenter requested clarification on the scope of physical access controls for BES Cyber System Information in Requirement Part 4.1.3. Physical access control for BES Cyber System Information only pertains to the protection of hard copies of said information. The hard copies of BES Cyber System Information are not required to be within a PSP, and therefore, CIP-006-5 may not apply.

Several commenters requested clarification on the phrase "within the last seven years." In order to obtain or retain access, a person must have had a personnel risk assessment "within the last seven years" of when access was provided and ongoing. The Requirement is written to be flexible to allow the entity to design and implement their personnel risk assessment program in a manner that meets its needs. For some, this may include performing personnel risk assessments more frequently.

Requirement R5

One commenter noted that Requirement Part 5.1 does not distinguish between termination for cause and termination without cause. The SDT removed the distinction between types of terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access regardless of termination reason.

There were an abundance of commenters that noted that the time frame listed Requirement Part 5.2 is difficult to comply with and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. The Requirement allows for the entity to review the access for the individual and retain access as long as necessary for transition from the prior position. The timing was determined to be necessary to meet the to meet FERC Order No. 706, Paragraphs 460 and 461, requiring immediate revocation for any person no longer needing access which includes reassignment and transfer. Note that the timing is based on when the entity determines that the individual no longer needs access, which may not necessarily be the same date as the transfer or reassignment.

One commenter requested clarification for the word "removal" in Requirement Part 5.1. Removal refers to rendering the individual unable to use the access. This may be accomplished through deletion, disabling, revocation, or removal. The SDT wanted to provide flexibility in allowing any of these means to be used.

A few commenters requested clarification regarding Requirement Part 5.4 on what scenarios would fall into this category that are not covered within Requirement Parts 5.1 to 5.3. Requirement Part 5.1 is removing the person's ability for unescorted physical access and Interactive Remote Access. This can be accomplished by revoking just these elements (i.e.: RSA, VPN, Active Directory). Requirement Part 5.4 is to clean up the remaining accounts for the users, such as access to applications, databases, and other systems.

One commenter had concerns that Requirement Part 5.5 could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people's ability to access BES Cyber Systems (they forget the password due to the high change rate). The SDT believes that due to the capabilities of these accounts, prompt changing of the password is appropriate to minimize the risk from separated employees and contractors.

One commenter requested that "termination action" be replaced with "termination" in Requirement Parts 5.1, 5.3, and 5.4. Please see the Guidelines and Technical Basis section of the standard for additional information regarding a termination action. This section addresses the concerns noted.

There was a request that the phrase "and time" be removed from Requirement Part 5.3, as it is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. The SDT agrees with that clarification and has modified the Requirement to address this comment.

One commenter considers the time limits for revoking access upon terminations to be an extreme challenge. The SDT used the timeline for terminations to meet FERC Order No. 706, Paragraphs 460 and 461, requiring "immediate" revocation for any person no longer needing access, including all terminations, and the SDT believes the approach reflected in the standards is a reasonable means of accomplishing the directive.

One commenter requested consideration of Requirement Parts 5.4 and 5.5 to include Physical Access Control Systems (PACS) since some cyber assets in a PACS can also have individual user and shared accounts. The SDT considers all PACS devices to be subject to the same Requirements, regardless of impact categorization. While removal of access and changing of shared account passwords on all assets is a good security practice, it is not a Requirement under the CIP version 5 standards except where noted in Requirement Parts 5.4 and 5.5.

One commenter requested that Requirement Part 5.5 be changed to 35 days for consistency with other monthly Requirements. The time parameter in this requirement is different than the periodic performance time periods in requirement parts that use the 35 calendar days period. The SDT does not consider this action to be an ongoing monthly Requirement similar to those noted in CIP-007-5.

CIP-005-5

High Water Marking

There was a comment that per the Guidelines and Technical Basis section for CIP-005-5 Requirement R1, all of the Cyber Assets and Cyber Systems, even other BES Cyber Systems of lesser impact, within the Electronic Security Perimeter (ESP) will be elevated to the level of the highest impact BES Cyber System present in the ESP. The commenter recommended that this concept be included in section 5 background of every standard, not just in CIP-005-5 guidance. The SDT considered whether to include this in the background in each standard, but determined that it was most appropriate to make clarifying changes to the Guidelines and Technical Basis section in CIP-005-5.

Background Section

One commenter suggested that to ensure consistency between the standard and the list of "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" to update this section to reflect the same definition as used in this list. In response, these do not change or modify the definitions, but provide further background and guidance information.

There was a comment in the Guidelines and Technical Basis section that stated that an ESP is required around networks even if standalone regardless of impact classification. The commenter ask the SDT to confirm the Requirement in CIP-005-5 do not imply a list of Low Impact assets is needed. In response, the SDT has added the word 'applicable' before BES Cyber Systems in the guidelines to clarify this.

A question was raised regarding the scenario where a network switch may be divided into multiple ESPs and has one port outside the ESP that provides no routing between VLANs. Furthermore, the commenter questioned the following regarding Requirement R1.5: "does two distinct machines need to be utilized, one as a fire, and one as intrusion prevention or can it be done via one device and when the EAP is segmented into multiple network where one LAN is critical and one is non-critical; and does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic." In response, the SDT is writing Requirements for the "what's" and leaving the "how's" to the entities to implement in ways that best protect their environments while still meeting the intent of the Requirement. These standards cannot and should not be exactly prescriptive in every possible technical situation. If that were the case, they would be constantly outdated or they would actually increase our risk by presenting a monoculture to adversaries where a vulnerability in one would be the same vulnerability in all. For the VLAN question, the SDT notes that an ESP (a logical border) is required around every network

to which a BES Cyber System is connected and any external connectivity to other networks must be controlled with an Electronic Access Point (EAP). The SDT has chosen to not prescribe precisely what protective functions must reside on what devices or what the standard network architecture must be for the reasons noted above. A method for detecting malicious communication must be present at each EAP for control centers (high and medium impact).

Consideration of Data Diodes

One commenter stated that CIP-005-5 should consider data diodes which possibly would exempt systems only with a data diode connection from "external connectivity" provisions. In response, the SDT notes that the definition of 'External Routable Connectivity' includes the term 'bi-directional' in order to handle data diode situations that physically enforce a uni-directional flow. Therefore systems behind a data diode do not have External Routable Connectivity.

Requirement R1

One commenter asked what the rationale was for standalone networks that have no external connectivity to other networks to must have a defined ESP. The intent is to define the 'Associated Protected Cyber Assets (PCAs)' and the high watermarking concept. In response, in previous versions of the CIP standards, Cyber Assets on the same network (within the same ESP) with a Critical Cyber Asset had to meet the CIP-007-5 Requirements. The definition of an ESP in Version 5 is required to carry this same concept forward, as well as to handle the new issue of what level of protection is required for these Cyber Assets now that we can have multiple impact levels within the same ESP. Therefore, if a BES Cyber System is connected to a routable protocol network, even an isolated network, the ESP (which is simply the 'logical border') must be defined as that also defines the 'Associated Protected Cyber Assets'. All of these Cyber Assets within that ESP then become 'Associated PCAs' of the highest impact level BES Cyber System in the ESP.

A commenter stated that the definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the Digital Protective Control Devices do not need to reside within the ESP and therefore are not subject to CIP standards. In response, the SDT notes that connectivity is no longer a filter that kicks Cyber Assets out of scope and makes them 'no longer subject to the CIP standards'. Cyber Assets are subject to the CIP standards based on their functionality and resultant potential impact to BES reliability. It is true that certain Requirements, such as CIP-005 Requirement R1, only apply if a BES Cyber System is connected to a routable protocol network, but that is because its main point is to secure what can enter or leave routable protocol networks on which BES Cyber Systems reside. CIP-005-5 is no longer a 'scoping standard' for what is or is not in scope of the CIP standards as a whole as it has been in the past. BES Cyber Systems are in scope of the CIP standards. CIP-005-5 Requirement R1

therefore is now back to a network security Requirement that requires controlling what can enter or leave a routable protocol network.

There was a comment that requested clarification text added to the Guidelines and Technical Basis section for Requirement R1, specifically Requirement Parts 1.3 and 1.5, to remove the operational barriers that may prevent entities from implementation encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. The commenter provided possible language to be added to CIP-005-5 Requirement Parts 1.3 and 1.5:

> "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within Physical Security Perimeters, the Requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 Requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced."

In response, The SDT believes the Requirements as written do not preclude the use of encryption. However, encryption alone does not constitute an ESP or EAP. For example, if malware is introduced via portable media to a BES Cyber System and it tries to communicate outbound to a command and control server to get further instructions or provide remote access to the BES Cyber System, the fact that there is an encrypted tunnel up to the next higher level site does not provide an EAP where the communications are inspected to determine whether they should be allowed or not. If an entity wishes to state that a wide area network of sites are within one ESP, regardless of encryption, then all Cyber Assets (which includes, e.g., all communication or networking equipment) within that very large ESP become associated PCAs and must meet the Requirements of the highest level BES Cyber System in the ESP. The standards do not preclude doing this, but there are implications that Responsible Entities should take into account.

For Requirement Part 1.2, one commenter stated that the definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. The commenter provided an example, where communication between two devices may take advantage of the Ethernet ports on the devices, but run serial

protocol between the devices. Furthermore, the commenter stated that by explicitly stating, "routable protocol connection" in the definition and focusing an auditor's attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Lastly, the commenter recommended deleting the word "connection" at the end of the definition of External Routable Connectivity. In response, the SDT disagrees. The definition is based on the type of protocol, not the transport used. Ethernet is not a routable protocol; it is a transport medium with no concept of network level addressing. It should not be assumed that transport determines protocol as routable protocols can be carried on serial lines and non-routable protocols can be carried on Ethernet. It is not a matter of transport but the protocol.

There was one suggestion in Requirement Part 1.3 that the term "permissions" can be substituted with the term "controls" to align the term with the language in the measure. In the measure, the SDT uses "access control list" as an example, and the SDT has not made a change to the Requirement language, as the use of "permissions" stems from prior versions of the CIP Cyber Security Standards. The SDT believes that the term is well-understood in this context.

One commenter had a concern with the phrase "outbound access permission" in Requirement Part 1.3 which calls for requiring inbound and outbound access permission, including the reason for granting access and denying all other access by default. The commenter furthered stated that target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled, and that while there is the possibility that could be malicious code internal to these networks communicating, that tracking all outbound communication from one trusted network to another trusted network would more than double the monitoring that is required. In addition, the commenter stated that the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. In response, the SDT does not think that having an outbound rule in an EAP that allows communication from all hosts on one internal network to all hosts on another internal network is burdensome. The benefit received of being alerted to BES Cyber Systems trying to suddenly communicate with unknown networks or hosts we believe outweighs the burden of such rules. The SDT is not prescribing the level of granularity of these rules. The intent is just that EAPs function as EAPs and don't have rule sets that allow a BES Cyber System to talk to any device in existence. The Requirement is in essence "you shall not blindly trust all hosts inside the ESP to talk to any device on earth". It is up to the entity how granular they control what the hosts inside the ESP can talk to. Some may go extremely granular and specify exactly what host can talk to what host over what port; some, due to the frequency of change or other reasons, may limit it to anything on this network can talk to anything on these other internal networks. Both are compliant. But BES Cyber Systems should probably not be able to communicate directly with all home PC's on the cable company's consumer broadband network or to any machine in unfriendly nations.

One commenter stated that Requirement Part 1.5 needed to include an explicit Requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. The SDT notes that monitoring and alerting is addressed in CIP-007-5, which also includes Electronic Access Control or Monitoring Systems (EACMS) (CIP-007-5, Requirement R4).

With regards to Requirement R1.5, one commenter proposed the following language: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. The SDT disagrees. If malicious code is trying to replicate itself from a primary control center to the backup Control Center, then this Requirement should be in place. Having both the primary and backup Control Centers compromised defeats the purpose. If the primary system is compromised via malware or remote control Trojans to the point that its integrity is gone and the entity needs to fail over to the backup while the primary is rebuilt, the backup needs this protection from the malware on the primary system. If the malware walked into the primary system via portable media or other means, an Intrusion Detection System (IDS)/ Intrusion Protection System (IPS) type system may save the backup system from compromise as well.

Another comment regarding Requirement Part 1.5 states that the Requirement is still geared towards implementing an IDS/IPS and that an IDS would not provide the additional protection for an ESP if a firewall failed. Also, the commenter noted that an IDS or IPS would provide no protection against an insider threat. The commenter closed by stating that “malicious” activity cannot be determined strictly by watching for an activity and that traffic to an ESP which is malicious may in fact appear to be normal. The qualification of “malicious” vs. “normal” requires knowing an actor’s intent, which cannot always be gleaned from log entries, traffic patterns or signatures. In response, the SDT has invested many hours in these very discussions and has arrived at the current Requirement. The Order makes it clear that the alternate control is also not simply another firewall. Having two firewalls in sequence would provide no value as the rule sets would be identical. The solution the SDT arrived at for an alternate control at an EAP was to detect malicious traffic (usually implemented in today’s technology via IDS/IPS as noted, but not prescribed). This would allow that if the firewall was misconfigured (e.g. an admin puts in a temporary any/any/all rule for troubleshooting and forgets to remove it after testing) then at least there would be this alternate control looking for malicious traffic and providing some means of protection which the SDT believes is the intent of the Order. As to the issue with “malicious” implying knowledge of an

actor's intent, the SDT has responded to this in previous drafts by inserting the words "known or suspected" to clarify that it is only malicious traffic that is previously known or suspected to be malicious.

Relating to requiring IDS and IPS to have firewalls, one commenter stated that it may be onerous compared to the benefit received. In response, the SDT disagrees. The SDT has already scoped this Requirement to the highest impact BES Cyber Systems which should be subject to the more stringent Requirements. The SDT believes that the benefit received from detecting malicious communications into and out of control centers far outweighs the burden.

One commenter asked for SDT clarification related to the ESP, External Routable Connectivity, and whether serially connected Cyber Assets are within scope for Requirements applicable to BES Cyber Systems with External Routable Connectivity. The SDT confirms that all BES Cyber Assets are in scope of all the CIP Version 5 standards. However, for certain Requirements, the type of connectivity limits applicability. EAPs for example, are only required around routable protocol networks to control what can get into and out of these networks. There is no EAP for a serial connection if there is no routable protocol running over it. Note that it is protocol based, not transport based. Routable protocols can run over serial transports. The same holds true for ERC – it is routable protocol based.

Requirement R1 VSLs

There was a comment that the language in the VSL should match the same language and logic as in Requirement R2. An example was provided that, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items, and thus, would result in a more consistent application throughout the standard. The SDT notes that it modified the VSLs for Requirement R1 in response to comments from draft 2 because of the difficulties and impracticalities of determining the measurements for graduated VSLs for Requirement R1.

Requirement R2

There was a clarification request for Requirment Part 2.2 with regards to allowing that encryption may be terminated at a firewall that protects an Intermediate Device in additoin to the Intermediate Device itself. The SDT believes that the definition of Intermediate Device provides sufficient flexibility in implementation to allow for what the commenter had requested. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. CIP-007-5 Requirement Part 5.1 refers to all user authentication; whereas CIP-005-5 Requirement Part 2 only refers to remote access.

There was a request that "where technically feasible" be added to Requirement Parts 2.2 and 2.3. The language "where technically feasible" is included in the overarching Requirement R2 to recognize that this applies to all of the Requirement Parts contained in Requirement R2, not just Requirement Parts 2.2 and 2.3.

Several commenters stated that CIP-005-5 Requirement Part 2.1 be modified to address situations where the Intermediate Device can be locally accessed (a local administrator, for example) inside the PSP. The SDT believes that, as currently written, the Requirement provides the level of protection necessary in that the Intermediate Device cannot be within an ESP and thus provides the necessary protection of the Cyber Assets within the ESP. The remaining controls for the Intermediate Device(s) provide a defense-in-depth proteciton of those systems. Additional references regarding the Intermedate Device are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter considered that CIP-005-5 Requirement Part 2.2 does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. The SDT notes that, as written, the Requirement and definition of Intermediate Device, collectively; provide sufficient flexibility in implementation to allow for what the commenter has noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 regarding the protections to be afforded to an "Intermediate Device". Per the definitions of Intermediate Device and Electronic Access Control or Monitoring Systems, these devices are subject to the protection of EACMS.

There was a request for clarification of CIP-005-5 Requirement Part 2.2 as to the reasonableness to include traffic between the "Intermediate Device " and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. Many instances of Interactive Remote Access originate from systems that are not within a trusted network or across the

Internet. The encryption is required to terminate before going into the ESP through an EAP. It is at the entity's discretion to design their Interactive Remote Access infrastructure and monitoring to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested that CIP-005-5 Requirement Part 2.2 be modified as "Interactive Remote Access sessions must utilize encryption to an Intermediate Device." The SDT believes that, as written, the Requirement language achieves the same concept and result.

A recommendation was made that CIP-005-5 Requirement Part 2.3 is modified as "Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

A request for clarification was made of CIP-005-5 Requirement Part 2.2 regarding whether the "Intermediate Device" is expected to provide the encryption or if two devices are envisioned for compliance. The SDT believes that, as written, Requirement and definition of Intermediate Device, collectively, provide sufficient flexibility in implementation to allow for what the commenters have noted. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested clarification of CIP-005-5 Requirement Part 2.3 on whether the multi-factor authentication is required for the Intermediate Device, for access to the EAP or to the individual Applicable Systems. The commenter suggested the language to read "Require multi-factor authentication for initiating all Interactive Remote Access Sessions." The SDT considered authentication to be necessary for the session, not for each device. The user may not actually log into each Intermediate Device itself.

One commenter requested clarification of CIP-005-5 Requirement Part 2.1 on whether VPN is an acceptable form of remote access. It is at the entity's discretion to design their Interactive Remote Access infrastructure to meet their specific needs. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There

are case examples showing differing implementations. Please see http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

CIP-006-5

General

There were comments that CIP-006-5 does not require an entity to define a Physical Security Perimeter (PSP) and wonders if entities must assume that it is required. In response, the SDT notes that access points to the PSP must be controlled, which by definition, requires the PSP. It is not necessary to have an additional Requirement stating the existence of a PSP.

Background Section

One commenter stated that the background section includes a definition/description of "Medium Impact BES Cyber Systems with External Routable Connectivity," that notes an exclusion in the following sentence: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." When this definition/description of Cyber Systems is used for the applicability in Requirements such as CIP-006-5 Requirement Parts 1.2, 1.4, and 1.5, it is used with the added inclusion of "and their associated...PCA." It appears the inclusive "and associated PCAs" statements in the Requirements negate the exclusion statement from the "Background," and makes the intended applicability of such physical security Requirements to specific Cyber Assets unclear for Cyber Assets without direct external connectivity which reside in the same ESP as Cyber Assets with direct external connectivity. In response, the exclusion in the background section states that it only applies to those Cyber Assets which are part of the BES Cyber System and not PCAs.

Requirement R1

One commenter stated that the deficiency correction language should not be added to CIP-006-5 Requirement R1 because it is a binary Requirement to either have a plan or not. The SDT notes that while the possession of a plan is binary, the implementation is not. Entities must document a plan with all of the applicable table parts and implement the plan at applicable BES Cyber Systems.

One commenter noted that the term "BES Cyber Systems without External Routable Connectivity" should be just "BES Cyber Systems". The SDT notes that "without External Routable Connectivity" is used to distinguish lesser obligations than those applying to "BES Cyber Systems WITH External Routable Connectivity".

Several commenters stated that CIP-006-5 Requirement R1 does not answer the question of how big an opening needs to be before it is considered an access point. In response, the SDT does not agree this question needs to be answered in a

standard's Requirement. This is an implementation-specific question. An entity may choose 96 square inches as its general measure, but that should not be the Requirement. Specifying exactly the qualifications of an access point would go beyond just the 96 square inch Requirement and likely cause significantly more confusion than currently exists.

One commenter did not agree Requirement Part 1.3 is responsive to the directive in FERC Order No. 706, Paragraph 573 to provide layered and complementary security procedures. In response, the SDT notes that in paragraph 575, the Commission specifically states it was not the intent to create an inflexible rule of redundant access control. The proposed Requirement meets the objective of having multiple physical access control measures. The Cyber Asset independence of these measures is not material to meeting the directive.

More than one commenter argued that Requirement Part 1.3 presents technical challenges without any additional security benefit. They request NERC to provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. In response, the SDT is addressing the directive in FERC Order No. 706, Paragraph 572. The SDT believes the proposed wording provides the most security benefit to the industry while still meeting the FERC directive.

One commenter suggested that for Requirement Parts 1.5 and 1.7 to remove the 15 minute maximum timeframe limit for issuing an alert. In response, the SDT notes that for physical security breaches, the threat is automatically severe and immediate and the 15 minute timeframe is necessary to provide a minimum expectation for issuing an alert.

One commenter proposed the words "of the unauthorized access" should be added to the end of Requirement Parts 1.5 and 1.7, but this would be redundant since detection is already qualified singularly in the Requirement Part.

There was a request for clarification if monitoring is needed on PACS inside a PSP according to part 1.7. In reviewing the possibility of combining Requirement Parts 1.5 and 1.7, the SDT found that monitoring and alerting Requirements applying to PACs could be interpreted to mean those inside a PSP. To clarify, the SDT notes that entities may choose for certain PACS to reside in a PSP controlling access to applicable BES Cyber Systems. For these PACS, there is no additional obligation to comply with Requirement Parts 1.1, 1.7 and 1.8 beyond what is already required for the PSP.

One commenter stated that in Requirement Parts 1.5 and 1.7, BES Cyber Security Incident Response Plan is not a defined term and should not be capitalized. The SDT agrees and has made this change. Furthermore, the commenter noted that unauthorized physical access should not automatically trigger the incident response plan because the physical security

team and incident response team are often separate groups, and a single instance of a detection of unauthorized physical access is not necessarily a Cyber Security Incident. The SDT notes that an attempt to compromise the PSP is by definition a Cyber Security Incident, and the organization of physical security and incident response teams should not preclude the Requirement to identify the Cyber Security Incident. The physical security team's response to unauthorized physical access could be part of the organization's incident response plan.

Several commenters stated that Requirement Part 1.7 should be modified to require response within 15 minutes of the detection rather than the actual incident, consistent with Requirement Part 1.5. The SDT agrees and has made the clarification.

One commenter proposed that Requirement Parts 1.5 and 1.7 be combined because they use similar wording, but the SDT believes entities benefit by emphasizing the applicability to PACS outside of the PSP.

There was a comment that stated that Requirement Parts 1.6 and 1.7 should include badge readers outside of the PSP and access cannot be controlled as specified. In response, these Requirement Parts are separated because they must be monitored differently than those Cyber Assets inside a PSP. The SDT also notes that badge readers, by themselves are not necessarily considered PACS if they do not control the controlling, logging or alerting of access.

One commenter noted that a responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no Requirement that the PACS be contained within a PSP. Therefore, a question was raised as to how does one control physical access to the PACS? In response, the SDT notes that PACS must control access according to Requirement Part 1.1, which is not the same level as Requirement Parts 1.2 through 1.5, but some form of access control must still exist for the entity.

Several commenters noted that Requirement Part 1.7 requires coordination with the incident response team, but CIP-008-5 does not apply to PACS. In response, the incident response plan does not apply to individual Cyber Assets, but compromise of a PSP and associated PACS is by definition a Cyber Security Incident affecting a BES Cyber System.

One commenter requested clarification on whether the issuance of an alert according to Requirement Parts 1.5 and 1.7 is automated, manual, or by choice. The SDT clarifies this is by choice of the entity.

There was a suggestion that there is a discrepancy between the change description stating PACS does not need to be inside a PSP and Requirement Parts 1.5 and 1.7 stating obligations for monitoring and alerting for unauthorized access to PACS. In response, Requirement Parts 1.2 through 1.5 applies to the BES Cyber System. PACS have a less stringent obligation in Requirement Part 1.1 to have a plan for restricting unauthorized access, but this is not the same obligation as having a PSP. The SDT has clarified the change rationale for Requirement Part 1.1.

One commenter stated that Requirement Part 1.8 should add "initial" before entry to align with the visitor control program. In response, the situation allowed for in the visitor control program is to avoid an escort continually signing in a visitor needing to perform a maintenance activity. This is not the same concern for authorized personnel who typically badge in each time without the overhead of an escort.

One commenter stated that Requirement Part 1.9 should be moved to data retention. In response, the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R2

There was a comment that the CIP Exceptional Circumstances should be removed since it applies globally at a policy level. In response, the CIP Exceptional Circumstance provision is controlled at a policy level but does not apply globally to all Requirements in the standard. The standards specify which Requirements the exception may apply to as a response to the FERC Order No. 706 beginning with paragraph 372, which directs additional guidance on policy exceptions.

Several comments stated that the Requirement could allow a visitor to go a long span of time without signing out. In response, the SDT notes the scenario of brief exit/entry intervals provided in comments is the purpose for allowing this provision. Specifying what timeframe constitutes the necessity of an exit sign-out goes beyond the security benefit provided by this Requirement Part.

Several commenters noted that the measure in Requirement Part 2.1 does not match the Requirement because the evidence does not demonstrate continuous access but discrete points in time. In response, the Requirement to have a program that provides continuous escorted visitor access can be measured by the program document. Evidence of compliance with the procedure requires discrete sampling to provide assurance in the implementation of the program.

One comment was that Requirement Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter and the Requirement for egress has not been explicitly defined as a Requirement. In response, egress logging has been required since CIP-006-3.

There was a comment that Requirement Part 2.3 should be moved to data retention. In response, R2.3 was not included as an evidentiary requirement. The SDT notes that the retention of these logs serves the reliability objective of having access logs to support incident identification and response.

Requirement R3

One commenter stated that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One comment was that the 24 month interval in Requirement Part 3.1 is excessive for a normally occupied control center. In response, a normally occupied control center would also receive a significant amount of testing in the operation of access control. The objective this Requirement primarily addresses field assets where access is not tested as frequently, and the timeframe is appropriate for these assets.

Guidelines and Technical Basis

Several commenters recommended modifying the section dealing with alarms to be from “immediately after” an incident to “within 15 minutes.” This better aligns with the Requirement and the SDT agrees.

CIP-007-5

General Comments

One commenter requested guidance on how to comply with CIP-007-5 Requirements on Medium BES Cyber Systems serially connected devices with regards to patching, anti-virus, etc. on a large number of programmable protective relays; and also why other measures implemented for substation assets, such as physical protection, are not adequate. In response, the SDT notes that BES Cyber Assets by definition can have an impact on BES reliability and therefore require basic cyber security protections offered by CIP-007-5 regardless of their connectivity. For patch management, the intent is that entities know about the security patches that are available for their BES Cyber Assets, what vulnerabilities they represent, and mitigate those vulnerabilities. If a security patch for a device is only exploitable over a routable protocol connection and the device is only attached serially with non-routable protocols, then that patch would be documented as not applicable. The anti-virus Requirements and guidance already mention that the entity is to document and implement how they protect against the introduction of malicious code to the BES Cyber System. For some of the devices in the example, the entity may document that there is no method to introduce malicious code.

Effective Dates

One commenter raised a concern that the effective date of the order providing applicable regulatory approval, and Requirement Part 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. In response, it is the intent of the SDT that the entity has the accounts inventoried on the effective date, not one year later. That is why there is a two to three year implementation period so that all these prerequisite activities have sufficient time to be completed so that the entity is fully compliant on the effective date. The Requirements that require periodic reviews may have their first performance take place after the effective date, but that is outlined in the implementation plan.

Requirement R1

One comment stated that a new term of “Control Center Environment” was introduced in this standard and it could potentially have a different meaning than “Control Center”. The commenter requested clarification, and in response, the SDT agrees and has changed the term to “Control Center.”

For CIP-007-5 Requirement Part 1.2, several questions were asked about the phrase, “Protect against the use of unnecessary physical input/output (I/O) ports used for network connectivity, console commands, or removable media.” Introduction of physical port protection is “assumed” to refer to logical ports only. First, a question was raised about

strong physical access controls to BES Cyber System be a compensating control here. Second, will having the BES cyber systems in locked cabinets suffice? The Requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the Requirement the way the Requirement is written. For CIP-007-5 Requirement Part 1.2, the commenter sought clarification regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language "console commands" is too ambiguous. In response, the SDT notes that many of these issues are addressed in the included guidance. FERC has stated that the PSP does not meet the intent of their Order. The SDT agrees with the 'console commands' comment and has added additional guidance to address it.

For CIP-007-5 Requirement Part 1.1, several comments were made about the phrase, ""If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The Requirement does not provide any provisions for limiting access to those ports or services that cannot be disabled. The Requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this Requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. In response, the SDT notes that the Requirement does provide provision for those ports and services that cannot be disabled which is the phrase in question. If a device has no provision for disabling or restricting the ports, they are deemed "needed" and the Requirement only requires "unneeded" ports to be disabled. The intent is to not require TFEs for devices where the device does not allow for the Requirement to be met. The Requirements in CIP-005-5 for limiting inbound and outbound communications at the ESP is a mitigating factor for devices like this that do not allow for their "unneeded" ports to be disabled.

Requirement R2

There was one comment that stated the rationale specified a 30 day time frame while the Requirement states 35 days. The commenter requested that the rationale section be revised for consistency with the Requirement language. In response, the SDT agrees and has changed the rationale to 35 days to agree with the Requirement.

One commenter suggested adding "with External Routable Connectivity" to the Medium Impact applicability for the patch management Requirements within Requirement Parts 2.1 through 2.4. As justification, the commenter stated that they understand the comments of the SDT; however, the commenter believes that a combination of no external routable

connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats ("thumb drives, laptops, smart phones") into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, a request was made that the timeframes for Requirement Parts 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. In response, while routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means in which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable. As to the 90 day alternative, the SDT believes that a timely analysis and plan are necessary due to the nature of the environment we are in where 'Patch Tuesday' is immediately followed by 'Exploit Wednesday' as attackers quickly reverse engineer released security patches to create and release exploit code. The SDT has not put a maximum timeframe on implementation due to numerous reliability concerns, but the analysis and mitigation planning needs to occur in a timely fashion.

There was a comment that Requirement Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. Furthermore, the commenter stated, *"the corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take*

appropriate interim action." In response, the SDT agrees with the concept; however, the SDT does not find it appropriate to prescribe in regulation certain 'timely' sources, including private firms, that must be used. Patch monitoring services can come and go. The SDT also believes that it should not use undefined terms such as 'timely' in a mandatory Requirement, nor should it define 'timely' as it refers to the seemingly unlimited number of patch sources that will exist with the significantly expanded scope of Version 5. The SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan.

For CIP-007-5 Requirement 2, part 2.1, a comment was made that the patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, Programmable Logical Control (PLCs), and other electronic devices that are part of the BES Cyber System and do not have network connectivity. In response, the SDT agrees that any Cyber Asset that meets the definition of BES Cyber Asset is included in the CIP-007-5 patch management Requirement regardless of connectivity and that is the intent. While routable protocol connectivity is a way that systems can be compromised, it is not the only way and in many examples today is not the primary way. Insider threats (intentional and unintentional, from both employees and non-employees, from both portable media and support laptops) are means by which systems are compromised today. Therefore the intent of this Requirement is to remain aware of the vulnerabilities in the BES Cyber Systems through the security patches that are released for them and analyze and mitigate those vulnerabilities. If a system has no connectivity and a security patch is released that can only be exploited via network connectivity, then that vulnerability is already mitigated and the patch is not applicable.

One commenter requested a definition in Requirement Part 2.1 for the phrase "applicable asset," and also suggested that the phrase "Applicable Cyber Asset" should be called "Applicable System" to align with wording in the column "Applicable Systems". In response, the SDT notes that individual BES Cyber Assets have patches, not systems of Cyber Assets. A system is a logical grouping of one or more BES Cyber Assets. While the applicability is at the system level, the Requirement is to perform patch management on all of the applicable BES Cyber Assets within those applicable systems.

There was a comment made on the change from 30 days to 35 days within Requirement Part 2.2. The comment was that this change allows utilities to manage patches monthly while coinciding with vendor releases, all without running into

issues of the Requirement being less than a full month. However, the commenter stated that this should be extended to 40 days to accommodate time to review the vendor releases, and that the additional five days on top of the existing 35 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. In response, the intent is for a process that approximates "monthly" and the SDT has already added in at least a four period to account for holidays, weekends, and other factors. The SDT does not agree that it needs further extension. Timely analysis of security patches is the goal.

Within Requirement Parts 2.2 and 2.3, one commenter requested clarification of the use of term "mitigation plan" and how it would provide value. To clarify Requirement Part 2.2 the commenter suggested mentioning that the mitigation plan is intended as an internal document and not submitted to the RE. In response, the SDT agrees and that these plans are internal documents and not submitted to the RE. In previous drafts, these were called 'remediation plans' and the SDT received comments that this term was used for what was submitted to Regional Entities in response to violations of the standard, so the SDT changed the term to 'mitigation plan' to avoid that confusion. The SDT has added this clarification to the guidance.

There was a comment with regard to CIP-007-5 Requirement Part 2.3 that reads, "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to "create a dated mitigation plan or revise an existing mitigation plan will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to "Develop dated implementation plan" without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability." In response, the SDT notes that the 'dated mitigation plan' could simply consist of the date the entity plans to implement the security patch if beyond the initial 35 day period; therefore it is not simply a paperwork exercise that provides no reliability benefit. The intent of the Requirement is to mitigate the applicable vulnerabilities either through the installation of the patch or by some other means. Implementation of the patch is mitigation and having a record of the entity's plan to implement the patch is not seen as unnecessary paperwork.

There was a comment that Requirement Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. Furthermore, the commenter stated "there are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no Requirement for

the CIP Senior Manager approval, thus allowing an entity to completely avoid the Requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This Requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this Requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required." In response, the SDT believes that the reliability of the BES will be better served by mandating that all vulnerabilities in all applicable BES Cyber Systems be known and analyzed by all entities than by trying to micro-manage what must occur with each system, patch, and vendor through a one-size-fits-all process. As stated in the guidance, patching systems can cause more risk to BES reliability than having a non-patched system in a given situation and the Responsible Entity, not the SDT, is in the best place to weigh these risks and develop an appropriate plan. The SDT has no way to write a mandatory Requirement for a "logical" plan.

One commenter believes that the language in Requirement Part 2.4 be aligned with the language in Requirement Part 2.3. The commenter suggests that either both or neither should specify the approval Requirement of the CIP Senior Manager of delegate. The commenter recommends that the language of "…timeframe specified in Requirement Part 2.3 is approved" be added. In response, the SDT notes the CIP Senior Manager approval was added to Requirement Part 2.4 specifically to handle situations where entities might repeatedly extend their documented timeframe with no management oversight. The intent was not to have management approval of every patch in normal day-to-day processes. Entities are free to do so, but it was not the SDT's intent to make that a mandatory Requirement. Management approval of every patch on every BES Cyber Asset would tend to become a "rubber stamp" with no meaning. The SDT's intent was to have approval of exceptions so that if someone were simply moving deadlines to avoid complying with the intent of the Requirement it would be subject to management oversight.

Requirement R3

There was a comment that within Requirement Part 3.1 to consider adding the phrase "per device capability" to the beginning of the Requirement, or otherwise, if a deter posture is selected, it may be potentially in conflict with other

Requirements. In response, the Requirement is written at the system level in order to handle the device-specific issues. The SDT believes the included guidance also provides suggestions on how to handle device abilities.

With regard to CIP-007-5 Requirement 3, parts 3.1, 3.2, and 3.3, there was a comment that these three Requirement Parts do not have any timeline for action. A question was raised if an auditor will audit when the activity occurred and audit only that a process is created and executed per the registered entities process or procedure. In response, the answer to the question is yes. Malware protection is an inexact art as we are protecting against an intelligent and always changing adversary. Malware of today is quite different than malware of just a few years ago. The intent is for entities to think about the malware problem, document what they are doing about it for each BES Cyber System, and then do it. Prescribing certain technologies/tools/timeframes is not helpful in this rapidly changing area and tends to bog the industry and the regulator down in paperwork (such as TFEs) when agility in this area is required in order to protect BES reliability.

Within Requirement Part 3.2, one commenter stated that the word 'identified' is ambiguous and inconsistent with other malicious code phrases, and the commenter suggested changing the language to 'detected'. The SDT agrees with this clarification and has made the suggested change as this is how the measures and guidance were written as well.

One comment was related to the applicability section of Requirement Part 3.2. A suggestion was provided to revise this section to apply to Medium Impact assets with external routable protocol to read: "Medium Impact BES Cyber Systems with external routable protocol and their associated". In response, the SDT's intent is for the basic security protections, including malware prevention, to be applied to all BES Cyber Systems not just those with External Routable Connectivity. BES Reliability can be threatened on isolated networks of BES Cyber Systems through the introduction of malware through portable media or laptops used for support.

One commenter requested clarification on Requirement Part 3.3 which requires the anti-malware updating process to address testing of the signature or pattern file. In support of this request, the commenter stated that a number of registered entities have taken the position in the past that they address this aspect of the existing CIP Version 3 Requirement by relying upon the vendor to test before release. In response, the Requirement is taken verbatim from previous industry and FERC approved versions of the CIP standards. If the entity is obtaining tested signature updates from their control system vendor for a turnkey product, then that is compliant. The SDT does not think more prescription as to where the testing must occur is needed.

There was one comment raised that use of the term 'deter' is ambiguous and the commenter suggested replacing this language in Requirement Part 3.2. The commenter suggested replacing the language to read: "Configure the measures implemented in Requirement Part 3.1 such that it blocks or prevents access to files with potentially harmful code." This recommendation was based on the assumption that the recommendation for removal of the term "deter" is accepted in Requirement Part 3.1. In response, the SDT has purposefully added the word 'deter' so that entities are not in immediate violation of the Requirement should zero day malicious code enter the environment. There are no 100% preventions, so the SDT has added this verb to allow for that. Antivirus software tools today do deter, but do not 100% prevent.

Requirement R4

One commenter requested clarification around the last two sentences of the guidance section. The commenter also stated that currently, an entity that neglects to enable logging would be in violation. Per the Background section, a sole instance of deficiency is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the guidelines seem to be relics of a previous draft which conflict with the new approach. In response, the SDT agrees and has rewritten the guidance to properly align with the Requirement.

One comment read that CIP-007-5 Requirement R4 for security event monitoring does not state any Requirements as to when the security events, particularly in Requirement Parts 4.1 (log events) and 4.2 (event alerts) are to reviewed, escalated, and mitigated. A question followed that asked if there are any Requirements for immediate action from the IT security personnel for detected failed access attempts, failed login attempts, or specific event alerts. In response, no, there are no prescriptive timeframes for response to alerts. The Requirement is to generate an alert for security events. Alerting someone to a condition is one thing, responding to the condition is dependent upon numerous variables that cannot be prescribed.

A recommendation was made to revise this Requirement to include the sentence from the guidance section, "that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment." The SDT's intent was not for the Responsible Entity to determine in totality the events to be logged, but that it must log the listed events at a minimum (subject to device capability). The Responsible Entity is free to log events above and beyond these and is encouraged to do so. However, the Responsible Entity cannot ignore the listed events.

As currently written, CIP-007-5 Requirement Part 4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. A suggestion was made to rewrite this Requirement to read, "for BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level…" In response, the SDT's intent is that if a Cyber Asset has a local log on the device, then it should be utilized. For example, a completely standalone and isolated substation relay should log security events internally if it is capable of such so that if it begins misoperating there is some log to go review on the device to see if/who/when someone has accessed it. The Requirement is not dependent on external connectivity.

In Requirement Part 4.3, one commenter suggested that this is a data retention Requirement and should not be a Requirement of the standard. In response, the SDT's intent is that this is not strictly 'data retention for the purposes of audit' Requirement, but an actual cyber security Requirement to have ready access to the past 90 days of logs for the applicable systems for quick determination of potential cyber causes of reliability-affecting events. Quickly determining whether a BES event could have had a cyber security cause is a reliability-focused Requirement and the primary way to do that is to have ready access to security event logs. Configuring a system to retain the past five minutes of security event logs is of little to no value. This is a separate issue from having evidence for audits that you maintained 90 days of logs throughout the audit period.

Within the Guidelines and Technical Basis section of CIP-007-5, Requirement R4, a question was asked if the following quotation references to NIST are the guiding principles and documentation for the development of the RSAWs and auditing of this Requirement, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." In response, these guidelines are not auditable, only Requirement statements are auditable. These are provided solely for use at the discretion of Responsible Entities, several of whom have asked in previous drafts for further guidance.

One commenter requested clarification on the word "review" with regard to the statement within Requirement Part 4.4 of "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." The commenter questioned if an automated SIEM technology solution, which monitors real-time, would satisfy the Requirement. In response, the SDT states that the intent, as per FERC Order No. 706, is to manually review the logged events in order to ensure that automated tools such as SIEM systems are tuned appropriately and are not missing security events.

One commenter stated that CIP-007-5, Requirement R4, part 4.1.2 calls out failed access attempts and failed login attempts and is unclear as to why the phrases "failed access attempts" and "failed login attempts" are separated. The

commenter requested clarification on the following two questions: Are “failed access attempts” referring to physical attempts, and are they referring to some other form of electronic access to undermine the login process? In response, the SDT notes that as outlined in the guidance, access attempts primarily occur at EAPs and involve ‘access’ across the ESP. Login attempts primarily occur at the BES Cyber Systems. The monitoring Requirement applies to both situations.

A comment was issued on Requirement Part 4.1.3 that this Requirement of malicious code prevention methods to log is already contained in Requirement Part 3.2. The commenter suggested removing this Requirement. In response, the SDT notes that logging and alerting when malicious code is detected is a separate Requirement from the actual response to the alert and the mitigation of the malicious code on the BES Cyber System. The SDT sees no duplication between these Requirements.

There was a comment that within CIP-007-5 Requirement Parts 4.2 through 4.4 the Requirements and sub Requirements have become less clear than previous CIP standards versions. The commenter stated it was unclear if Requirement Part 4.4 replaces the previous monitoring Requirements in their entirety or if it represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. The commenter suggested to consider modifying the aforementioned Requirements to make it clear to registered entities which logging is required, how logs should be monitored, and what actions are required in the event of an interruption in logging. In response, the SDT notes that Requirement Part 4.4, as noted in the Rationale and Change Justification, is in response to FERC Order No. 706 and the Directive to require a manual review of logs to insure that automated tools are not missing events. Automated tools are only as good as their rule sets, which require periodic tuning.

One commenter noted that a clarification may be needed for Requirement Part 4.2 as to whether the alert needs to be generated real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. In response, the SDT’s intent is, in general, for a real-time alert, but the SDT did not specify that as a timeframe in the Requirement because, for example, an after-the-fact review or analysis of logs would not require a computer-generated alert.

One commenter stated that Requirement Part 4.2 is a questionable and subjective Requirement as it states that an entity needs to generate alerts for security events that the entity determines necessary. In response, the SDT has set a minimum threshold of alerts that must be generated if the system is capable of it. All other types of alerts vary widely by the type of system in question and should not be prescribed. The alerts that can be generated by a Windows or Unix

server in a data center are quite different than what can be generated by some legacy purpose-built device in a substation.

A request was made to clarify Requirement Part 4.3 as to whether original source logs must be retained or if post-log analysis summaries are sufficient. In response, the SDT states that the language in the Requirement and measure provides the necessary level of clarity.

There were several comments on Requirement Part 4.4 that need to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. Similarly, another comment for CIP 007-5, R4.4 read, in the Requirements column of the table, the draft language indicates a need to review logs to, "identify undetected Cyber Security Incidents." A question was raised if this is intended to be "identify detected Cyber Security Incidents?" Also for CIP-007-5 Requirement Part 4.4, a recommendation was made to change "undetected" to "potential". In response to the aforementioned comments, the SDT notes the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

One comment read that in Requirement Part 4.4, to be consistent with other Requirements, that the phrase "15 days" be changed to "15 calendar days." In response, the SDT agrees with this clarification and has made the change.

A recommendation was provided to change the language in Requirement Part 4.2 to read "Detected failed login attempts from part 4.1." In response, the SDTs intent is that alerts be generated when it is detected that event logging has failed.

One commenter raised an issue that in Requirement Part 4.4 the words "summarization" and "sampling" components are too broad. In support of this, the commenter encouraged specificity in all measures. Additionally, the term "undetected" is unclear and confusing. The commenter stated that clarification, such as "logged but not previously selected for alerting or alarming" could be helpful. In response, the SDT has chosen to not provide further prescription but to use the words from FERC Order No. 706 to allow entities to meet the intent without prescribing exactly how to summarize or sample

the logs. Sufficient summaries or samples are dependent on many variables and do not lend themselves to a one-size-fits-all approach.

A comment was made with regard to Requirement Part 4.4 that a manual log review is a labor intensive and outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review processes for this Requirement. The commenter believes that this Requirement is ambiguous. The commenter further stated that the Requirement to review 'undetected' Cyber Security Incidents is essentially a Requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the Requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. In response, the SDT has added this Requirement in response to a directive in a FERC Order. The intent is to ensure that such automated tools are continually tuned and are not missing events that should be caught and alerted on.

A request was made to clarify Requirement Part 4.4 that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. Furthermore, the commenter stated that the purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. With regards to the Requirement column of the table for Requirement Part 4.4, the draft language indicates a need to review logs to "identify undetected Cyber Security Incidents". Is this intended to "identify detected Cyber Security Incidents"? One last comment was a suggestion to change the word "undetected" to "potential". In response, the SDT states that the intent is to review logs to insure that any automated tools or processes are tuned so that they are catching all Cyber Security Incidents, therefore the SDT believes that the 'undetected' word is correct. If attempts to breach the security of a BES Cyber System are being missed because the automated tools are not tuned or maintained, then this Requirement's intent is to catch that.

Requirement R5

There was a comment that the TFE language in CIP-007-5 Requirement Part 5.6 is unnecessary since technical or procedural controls can be used and that the phrase "per Cyber Asset capability" be used instead. In response, since many Cyber Assets used today utilize shared accounts and have no capability for individual accounts, periodically changing passwords is necessary. The SDT is aware that some systems have passwords that cannot be changed, or that if changed will break the system's functionality. Therefore, the SDT allowed for TFE's since the entity may not be able to

change the password either technically or procedurally. The SDT chose not to use the 'per Cyber Asset capability' as this is an instance where documenting and implementing some alternative control is necessary.

Within the Rationale section of CIP-007-5 Requirement R5, there was a suggestion to add the phrase “mimic display” to the second paragraph which outlines what is not included in interactive user access. In response, the SDT disagrees because the definition agreed to by the SDT is very clear and by adding another example with a non-widely used term would not add further clarity.

One commenter asked how CIP-007-5 Requirement Part 5.1 and CIP-005-5 Requirement Part 2.3 differ. The commenter stated that both appear to require authentication of Interactive Remote Access sessions. In response, CIP-007-5 Requirement Part 5.1 refers to any user access, including local access while physically present at the device. CIP-005-5 Requirement Part 2.3 refers to remote access.

A commenter believes that including specific password Requirements within a standard is contrary to new and safer technologies by the industry. In response, the SDT notes that the password Requirements have been worded in such a way that they only apply if passwords are used for authentication. If other, stronger means of authentication are used (tokens, biometrics, etc.) then the password Requirements do not apply. The Requirements are only “for password only authentication”.

One commenter stated that the term “generic account types” used in Requirement Part 5.2 is not defined and has not been well understood by entities to date. In response, the SDT notes that the term is now “default or generic” and the guidance provides some further explanation. The SDT does not believe that there is a sufficient definition of “generic” that will add any value beyond its normal dictionary definition.

One commenter suggested that within Requirement Part 5.2, alternate wording be provided to specify “known” enabled default or other generic account types. In response, the SDT agrees and has made the recommended clarification. The SDT notes this concept was already included in Requirement Part 5.4 and has included it here in Requirement Part 5.2 as well.

One commenter stated that Requirement Part 5.4 needs to be clarified that it pertains to active user accounts. The comments stated that there is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The commenter requested that the Requirement should also be clarified to require the initial

password change prior to placing the BES Cyber Asset into service. In response, the SDT disagrees. A known, published password should be changed even if the account is disabled. If the account is accidentally re-enabled, the password would be widely known. The SDT agrees that it would be a good practice to not only change the default password but also disable the default accounts if feasible, but it is not a Requirement.

There was a comment with regard to Requirement Part 5.4 that the word 'known' is ambiguous. For clarity, the commenter suggested changing the phrase "known default passwords" to "knowable default passwords". In response, the SDT disagrees that changing "known" to "knowable" solves the issue. The Requirement applies to the Responsible Entity, therefore it is "known to the Responsible Entity". Some vendors include "back door" user accounts in devices that are known only to the vendor and not the Responsible Entities. The Requirement is for the Responsible Entity to document only those that they know of.

A commenter suggested that Requirement Part 5.5's limitation to "password only" authentication is too narrow in scope and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. The commenter also stated that this would need to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). Another comment to Requirement Part 5.5 was that the first paragraph uses the phrase "interactive user access" and that this is not a defined term. However, it is similar to the CIP Version 5 definitions defined term. The commenter questions whether the phrase "interactive user access" should be defined or clarified in the Guidelines and Technical Basis section. The SDT has added language clarifying "interactive user access" from the rationale for Requirement R5 to the Guidelines and Technical Basis section for Requirement Part 5.5.

One commenter recommended that the phrase "…at least once every 15 calendar months" be replaced with "at least once each calendar year." In response, and as described earlier, the SDT disagrees as it has standardized throughout the CIP standards that the original use of the word 'annual' be replaced with 'once every 15 calendar months.'

With regard to Requirement Part 5.7, one commenter requested a clarification to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. In response, the SDT disagrees that a prescriptive number of attempts is warranted. The entities will be in a better position to determine how many attempts in what time interval are needed for the particular situation. There may be widely varying circumstances to take into account such as is the login used by a process that is vital and will locking it out or slowing the interval between tries affect reliability.

CIP-008-5

General

One commenter stated that both CIP-008-5 and CIP-009-5 have plan update Requirements and should be considered for removal. In response, the SDT does not agree these should be removed in this version because we address multiple Directives in FERC Order No. 706 related to the update of plan documents.

Requirement R1

One commenter suggested adding "assess" to the required processes in Requirement Part 1.1. The SDT does not agree there is a need to include "assess" in the Requirement Part.

One commenter recommended increasing the one hour reporting threshold in Requirement Part 1.2. In response, the SDT uses this timeframe to respond to a directive in FERC Order No. 706, Paragraphs 673 and 676. The one hour also refers to the preliminary reporting required from the point at which the entity has determined an incident is a Reportable Cyber Security Incident.

Several commenters suggested that the obligation to report to the ES-ISAC in Requirement Part 1.2 may not be acceptable for some Canadians, but the SDT is unaware of any ES-ISAC reporting restrictions for Canadians. However, the SDT has clarified that such reporting to ES-ISAC is only required, unless prohibited by law, to account for scenarios where federal or provincial laws may prohibit such action.

Several commenters stated that notification of the ES-ISAC occurs only after a Cyber Security Incident is determined to be reportable and the one hour timeframe should start at the determination of the incident as being Reportable. The SDT has modified the Requirement to clarify the one hour timeframe is from determination rather than identification.

One commenter requested clarification on the term "preliminary notice." In response, we quote from the Technical Guidelines section of CIP-008-5, "This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a Web-based notice. The standard does not require a specific timeframe for completing the full report."

There was a comment that the one hour timestamp in Requirement Part 1.2 would require a paperwork intensive burden on the entity that may qualify for removal according to Paragraph 81 of FERC's Order on the Find, Fix, and Track process.

In response, while additional documentation may be necessary to demonstrate compliance with the timeline, the objective this Requirement goes beyond an administrative function.

One commenter suggested changing the one hour reporting threshold of Requirement Part 1.2 to 24 hours to align with EOP-004-2. In response, the one hour threshold is directed as a change in FERC Order No. 706;the SDTs for both CIP Version 5 and EOP-004-2 agrees this obligation was best left in the context of CIP-008-5.

One commenter stated that the roles and responsibilities of the incident response plans specified in Requirement Part 1.3 should be left to the Responsible Entity. They expressed concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective incident response plan.

Requirement R2

One comment read that Requirement R2 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R2 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter proposed Requirement Part 2.1 needs clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be a disincentive. Regardless, it is best left to the entity to determine how to test its plan.

There was a suggestion that the testing periodicity in Requirement Part 2.1 is inconsistent from the period used across other standards. The SDT agrees and has made this modification.

One commenter proposed adding wording to confirm a single incident response plan is sufficient for all High and Medium Impact BES Cyber Systems. In response, the Requirement Part does not preclude having a single plan, and the rationale in Requirement R1 suggests doing so.

One commenter suggested that documentation of a Reportable Cyber Security Incident suffers a “catch-22” in that one of the steps is a determination of whether or not an incident is Reportable. In response, the documentation of a Reportable

Cyber Security Incident can be performed after-the-fact. This is not a Requirement to document each step contemporaneously with each action.

One commenter recommended removing the documentation of deviations in Requirement Part 2.2 since it is mostly captured in the lessons learned. In response, the lessons learned activity likely will use documentation captured from the Cyber Security Incident, but there is no obligation to document the use of the plan. The SDT chose to use documentation of deviations because this is a much less documentation-centric activity than documenting how the plan was used.

Several commenters stated that Requirement Part 2.3 should be moved to data retention. In response, the retention of this information serves the purpose of supporting follow-up incident analysis and correlation activates. There is otherwise no obligation to retain this information.

Requirement R3

There was a comment that Requirement R3 should have the language allowing an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter stated that CIP-008-5 Requirement R3 should allow deficiency correction. In response, the SDT does not agree this Requirement meets the criteria to be considered as high frequency, zero tolerance obligations as are the other Requirements that allow for deficiency correction.

There was a comment that in Requirement Part 3.1.2, lessons learned do not always trigger a plan update and that a qualifier “as applicable” should be added. The SDT agrees and has added the clarification, “lessons learned associated with the plan.” Corresponding changes have also been made in CIP-009-5.

There was a proposal that the timeframe in Requirement Part 3.2 could be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

One commenter proposed removing Requirement Part 3.2 or specifying only the affected roles and responsibilities. In response, the SDT notes that notification of all individuals is necessary for communication during a Cyber Security Incident.

One commenter stated for Requirement Parts 3.1 and 3.2, the wording needs to be rearranged to read better - the phrase 'no later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this change.

CIP-009-5

Requirement R1

One commenter stated that the roles and responsibilities of the recovery plans specified in Requirement Part 1.2 should be left to the Responsible Entity. They express concern for an auditor determining certain roles were left out of the plan. In response, the Requirement Part does not specify which roles must be in the plan, but having roles and responsibilities is a necessary part of an effective recovery plan.

There was a comment that Requirement Part 1.2 discusses responders without any additional clarification of who fits into this category. In response, this language has been carried forward from previous versions and the SDT has not received any additional comments supporting modification. The SDT agrees additional guidance would be helpful and has added clarification in the Technical Guidelines section of CIP-009-5.

There was one comment that stated that there should be more consistency in the applicability column of the tables and requests clarity on what applies if a Medium Impact BES Cyber System does not have a connectivity qualifier. In response, the lack of a qualifier only means that all Medium Impact BES Cyber Systems are applicable.

One commenter requested clarity on the intended frequency of performing Requirement Part 1.4. In response, the frequency is determined by the Responsible Entity. Some cyber systems may require a daily backup while other cyber systems, for example, at a power plant, may only require backups after major changes to the system.

One commenter suggested removing “and to address backup failures” from Requirement Part 1.4 because it may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. In response, the SDT notes that addressing backup failures meets the objective of the Requirement and purpose for verifying the successful completion of backups. Without this obligation, an entity could simply perform validation testing without performing any corrective action on the backup process.

Several commenters proposed changing Requirement Part 1.5 to “One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery.” However, the rephrasing has a subtle change in meaning. The per device capability exception applies to the preservation of data and not the procedure itself.

One commenter stated that Requirement Part 1.5 can lead to delay in recovery operations, particularly in a Control Center. In response, the SDT notes the provision of the Requirement that data preservation should not impede recovery.

One commenter requested clarification of Requirement Part 1.5. They state that it would seem the activity would delay recovery. In response, planning to preserve evidence could include additional individuals assisting in the recovery or retaining failed Cyber Asset equipment during recovery operation.

One commenter suggested adding a CIP Exceptional Circumstance qualifier to Requirement Part 1.5. In response, the SDT removed this qualifier based on industry comments because an event triggering recovery could most likely be a CIP Exceptional Circumstance, and thus nullify the Requirement. However, Requirement Part 1.5 achieves the same objective in having a qualifier to avoid the disruption of restoration activities. The commenter also expressed concern about the intent of Requirement Part 1.5 and suggests moving this to CIP-008-5. In response, the objective is to have this performed in any recovery operation and not just Cyber Security Incidents.

There was a comment for Requirement Part 1.5 suggesting that the Requirements could put the registered entity into a "catch-22" scenario where it could try to comply with the Requirement by saving logs, which might impede recovery. In response, the plan should address the issue where saving information impedes recovery as indicated in the Requirement Part.

One commenter stated that in Requirement Part 1.5, the device capability should be worded to clearly qualify the preservation of data. The SDT agrees and has made this change. They also suggested the measure be updated to include the device capability qualifier. However, the qualifier itself only applies to the Requirement and does not need to have inclusion in the measure.

Requirement R2

There was one comment that the words 'between tests of the plan' are not needed. The SDT agrees and has made this clarification.

One commenter requested clarification on how an entity tests a representative sample of information if, per Requirement Part 2.1, they performed a paper drill. In response, the SDT notes that the test in Requirement Part 2.2 is not necessarily the same test performed in Requirement Part 2.1.

One commenter proposed Requirement Parts 2.1 and 2.3 need clarification on whether a plan with multiple scenarios needs to have each scenario tested. In response, the SDT does not agree this clarification is necessary. It could be a benefit to consider multiple scenarios, and imposing a Requirement to test each would be disincentive. Regardless, it is best left to the entity to determine how best to test their plan.

There was a request for clarification on the difference between 2.1 and 2.3 and for additional guidance on what types of operational exercise the SDT considers meeting the Requirement. In response, the SDT refers to the Technical Guidelines section of CIP-009-5, which states "The HSEEP lists the following three types of operations-based exercises: Drill, functional exercise, and full-scale exercise. It defines that, '[A] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, Emergency operation centers, etc.) and 'boots on the ground' response (e.g., firefighters decontaminating mock victims).'"

One commenter suggested that Requirement Part 2.2 needs to provide additional clarification for a "representative sample" of information used to recover BES Cyber System functionality. In response, the SDT does not think it provides a benefit to further specify a representative sample of information in this Requirement. Otherwise, this Requirement becomes focused on the sample of information rather than the recovery of information. As specified in the rationale, "Requirement Part 2.2 provides further assurance in the information (e.g. backup tapes, mirrored hot-sites, etc.) necessary to recover BES Cyber Systems. A full test is not feasible in most instances due to the amount of recovery information, and the Responsible Entity must determine a sampling that provides assurance in the usability of the information."

A clarification request was made on Requirement Part 2.2 regarding a representative sample. The representative sample must be determined by the Responsible Entity. It could be a test of all the most recent backup tapes or it could be a single representative test for multiple instances of the same system.

Requirement R3

There was a comment that this Requirement should include language that would allow an entity to identify, assess, and correct deficiencies rather than self-report violations during CIP Exceptional Circumstances. However, the purpose of the self-correction provision is not intended to address CIP Exceptional Circumstances and the performance of Requirement R3 does not hamper emergency operations in a way that a CIP Exceptional Circumstance would be needed.

One commenter suggested that a lessons learned activity should not be required for every failure of equipment in the field. In response, failure of equipment in the field does not indicate a recovery operation in all cases.

There was a proposal that the timeframe in Requirement Part 3.2 be extended to 90 calendar days consistent with 3.1. The SDT notes that Requirement Part 3.1 also includes the lessons learned obligation so the cumulative time to update should be longer.

There were several comments on parts 3.1 and 3.2 that the wording needed to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. The SDT agrees and has made this clarification.

Guidelines and Technical Basis

One entity commented that the guidelines state that recovery plan information is BES Cyber System Information, which is not consistent with the definition of BES Cyber System Information. The SDT agrees and has modified the guidance to state that recovery plan information may be considered BES Cyber System Information.

CIP-010-1

Timeframes for Configuration Control Activities

The SDT received comments that the timeframes for configuration control activities are inconsistent. The SDT believes that the timeframes specified are consistent and are reflective of a reasonable configuration change control process.

Cross References to CIP-005-5 and CIP-007-5 on Impacted Controls

Comments expressed concern over the cross-reference to CIP-005-5 and CIP-007-5 as it related to the controls that could potentially be impacted by a change. The commenter recommended that the Requirement be broadened to include any control rather than simply those included in CIP-005-5 and CIP-007-5. The SDT appreciates the concern expressed in this comment and wrestled with this issue itself. After changes to this issue during multiple rounds of industry comment, the SDT believes that bounding the controls that need to be assessed is the most auditable approach.

The SDT received comments regarding a concern over double jeopardy between CIP-005-5, CIP-007-5, and CIP-010-1, specifically as it relates to the documentation of logical network accessible ports. The SDT does not believe this is a double jeopardy situation. CIP-005-5 and CIP-007-5 specify how ports are to be configured whereas CIP-010-1 specifies that they be documented.

Requirement R1

The SDT received numerous comments to add the “external routable connectivity” qualifier to the applicability section in Requirement R1. The SDT appreciates the concern regarding the amount of effort involved in maintaining baseline documentation for disconnected Cyber Assets. However, since these devices are disconnected, the point in time at which the device is interacted with is the only time that the configuration may actually be validated. Given this, the SDT believes it is worthwhile to formalize the configuration change management process for these systems such that an understanding of the current configuration of the device is assured at all times.

One commenter identified confusion as it relates to comma usage in CIP-010-1 Requirement Part 1.5.1. The SDT has clarified the Requirement and removed the incorrect comma.

One commenter asked for clarification that the items in the baseline are “current” and not historical. The SDT confirms that it expects that the baseline is a current representation of the configuration and that this should be kept up to date by Requirement Part 1.3.

One comment from industry asked for clarification as it relates to Requirement Part 1.4.2 and whether this verification that security controls are in place was to be performed on the production system itself. The SDT clarifies that this is the case. The intent of the Requirement is to ensure that the production system is properly protected following a change that affected its baseline configuration.

Several commenters asked for clarification on the use of TFEs in Requirement Part 1.5 (testing of changes) and whether the SDT actually meant CIP Exceptional Circumstances. The SDT envisioned that operational issues may prevent the ability to test a change prior to its implementation. The SDT believes that the TFE process provides the protection necessary to ensure that violations are not issued for a wide range of circumstances, including but not limited to those operational issues contemplated in the CIP Exceptional Circumstances definition.

Requirement R2

Comments expressed that the IAC language should be removed from CIP-010-5 Requirement Part 2.1 because this Requirement was itself an internal control. The SDT agrees that the Requirement represents a control; however it believes that, particularly given the required periodicity, that there could be deficiencies identified in the control itself and it therefore warranted the IAC language.

Requirement R3

One commenter recommended that the language in Requirement Part 3.3 be modified to add the word applicable ("Prior to adding a new applicable Cyber Asset...") in order to clarify that this Requirement did not apply to those systems that are temporarily connected for less than 30 days. The SDT agrees that this is consistent with the intent of the language and has modified the language accordingly.

The SDT received concerns regarding the performance of active vulnerability assessment prior to the deployment of new BES Cyber Assets. The SDT agrees that these assessments may be imperfect and that there may be some applications that will not properly function outside of a full production environment. However, the SDT continues to believe that since this is the only time when active scans may be safely performed on future production equipment that it is in the best interest of the BES for an active vulnerability assessment to be performed.

The SDT received comments preferring additional specificity as to what to validate during a vulnerability assessment. The SDT appreciates these concerns, but believes that a vulnerability assessment for an EMS system may look substantially

different from an assessment of a PLC. The SDT believes that the best approach is to allow the entity to define an appropriate assessment methodology for their environment, which may then be evaluated by an auditor.

The SDT received comments that questioned the technical feasibility of monitoring for changes to the baseline configuration. The SDT originally had intended for this monitoring to occur on a more frequent basis, potentially real-time monitoring. However, it was persuaded that there are some systems for which real-time monitoring would be infeasible. The SDT does believe that given the relatively high level items included in the baseline, that periodic monitoring every 35 days is a reasonable method to ensure that changes are not taking place outside of an entity's change control program.

Numerous commenters expressed concern about the Requirement to document the differences between the test and production environments. The SDT reminds the industry that this Requirement was the result of a FERC directive. Additionally, the SDT reminds the industry that it believes that for a relatively stable testing environment, that this documentation could be done once and utilized for multiple changes or testing cycles.

Commenters asked questions about the multiple timeframes for the vulnerability assessments for high impact BES Cyber Systems. The SDT confirms that these time frames are intended. Effectively, this requires an annual paper or active vulnerability assessment, but an active vulnerability assessment must be performed at least every three years. The SDT believes that the confusion raised by the question is due to the reader not considering the entire table as itself a single Requirement.

One commenter expressed confusion on the applicability of CIP-010-1 to access points. The SDT clarifies that since access points are the point at which access is controlled, they are included in the definition of EACMS and as such are applicable to CIP-010-1.

One commenter asked for clarification that the test environment did not have to be an exact mirror of the production environment. The SDT confirms that this was the intent of using the phrase "models the baseline configuration."

CIP-011-1

Requirement R1

Commenters requested that Requirement Parts 1.1 and 1.2 of CIP-011-1 Requirement R1 be clarified to indicate that a single method or procedure was sufficient. The SDT agrees that this is the intent and has clarified the standard as requested.

Commenters suggested that CIP-011-1 Requirement Part 1.2 should contain a measure that indicates "repository or electronic and physical location designated for housing BES Cyber System Information in the entity's information protection program." The SDT does not see how a repository is evidence of a procedure to protect and securely handle BES Cyber System Information. The SDT agrees that an information repository may be used effectively to meet this Requirement, but it is only a component of the evidence based upon a particular manner of implementation.

Requirement R2

One commenter requested that Requirement R2 of CIP-011-1 be moved to CIP-010-1 as it could be considered part of a change control process. The SDT believes that the objective of this Requirement is the protection of the information in a BES Cyber System and therefore believes it is appropriate to include in CIP-011-1.

Commenters identified a typographical error in the measure of Requirement Part 2.2. The SDT appreciates this correction and has updated the standard.

Implementation Plan

Effective Date

Several commenters had questions or concerns about the Version 3 to Version 4 to Version 5 transition within the standards' implementation plan. Some questioned whether extending Version 3 to the effective date of Version 5, and superseding Version 4, is still possible, while others asked for a deadline for accomplishing such a transition plan. The SDT appreciates these concerns, as they are issues of efficiency, planning, effort, and cost for all of the industry. However, the SDT also acknowledges that not all entities are situated exactly the same. As such, the SDT is hesitant to provide a "deadline" or other trigger for FERC action that would serve to foreclose the opportunity for the implementation language to be adopted in time to implement moving directly from Version 3 to Version 5. The SDT expects that the filing will address this issue in a manner such that certainty about the issue may come as soon as possible, and that the filing and other coordination between NERC and FERC is the appropriate venue for supporting the implementation plan after industry approval. In the meantime, it is reasonable to expect that some entities may need to make a risk-informed judgment to proceed with Version 4 implementation by a certain date if the proposal in the implementation plan is not approved expediently. Some entities may be able to wait longer than others into 2013 before making that determination. The SDT has communicated directly with NERC to underscore the importance of coordination of this effort, and the SDT believes that having an approved set of standards, definitions, and implementation plan before the end of 2012 continues to provide a reasonable timeline to consider the implementation plan proposal.

There was one comment that 36 months to comply with CIP-003-5 Requirement R2 is excessively long since it only requires documentation of a few policies. The SDT notes that CIP-003-5 Requirement R2 requires implementation, and not just documentation of policies. This expands to a significantly large number of the overall reported BES Cyber Systems, which warrants such a timeline.

One commenter suggested that it misleads entities to allow the provision suspending compliance with Version 4. The SDT does not agree this is misleading. The SDT has been careful to communicate the risk in awaiting this order to begin planning compliance with Version 4. Furthermore, the FERC approving this provision, even if it is closer to the Version 4 Effective Date, still spares entities and auditors alike untold expenses of a compliance monitoring program for Version 4.

A few commenters asked about audits in 2015 during the expected transition window to Version 5's effective date. That is outside the scope of the SDT, but the SDT has tried to account for a smooth transition within the implementation plan,

to include specifications for initial required performances of periodic events. In response to this question and the issue of transition from Version 3 to Version 5, the SDT understands that NERC is preparing information to assist in the smooth transition among CIP standards versions, and that such information will be coordinated upon certainty that Version 5 has been approved by the industry and is no longer subject to change.

One commenter stated that the effective date language should be qualified with a statement that sufficient time should be given for completion of CIP-002-5 R2 to comply with CIP-003 through CIP-011. The SDT believes this is already well understood and ongoing communication and training will provide entities further guidance to categorize BES Cyber Systems with sufficient time to comply with CIP-003 through CIP-011.

Several entities comment that NERC and the drafting team should request FERC to suspend compliance with Version 4 and allow entities to transition from Version 3 to Version 5 on the effective date. In response, the proposed effective date does bypass Version 4 and provides the FERC the opportunity to issue an order approving this provision. In effect, this is the industry and SDT communication to the FERC requesting the bypass of Version 4.

There was a comment that suggested extending Version 3 until Version 5 becomes effective could not be accomplished in Canada through an implementation plan. In response, the SDT notes that Canadian jurisdictions would be subject to the second provision for "those jurisdictions where no regulatory approval is required." The commenter is correct that the proposal in the Implementation Plan, if approved, would supersede any other Order to the contrary. In all cases of reliability standards, the Implementation Plan is subject to regulatory or other applicable federal approval.

A few commenters noted that CIP-003-5 is dependent upon CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1 passing. The SDT confirms the commenters' understanding and notes that the implementation plan conditions all standards passing before any of them become effective.

One commenter expressed concern that the implementation of CIP-004 through CIP-011 should be combined into those standards. The SDT points out that the implementation of security procedures in CIP-004 through CIP-011 is included in those Requirements that have actions associated with them. The entity should refer to the high level Requirement for the implementation language.

Initial Performance of Certain Periodic Requirements

Several commenters stated some confusion with the initial performance of periodic Requirements section or suggested that it is unnecessary and, if retained, should be in guidance. The SDT notes this section was incorporated from industry comments, and moving this section to guidance would be misleading because the additional time for compliance with periodic Requirements would not be enforceable in guidance.

There was a comment that no provision for CIP Exceptional Circumstances exists for some periodic Requirements and that an entity should be allowed to track instances of non-compliance in CIP Exceptional Circumstances rather than self-report. In response, the SDT has indicated where exceptions may occur to the standards in defined CIP Exceptional Circumstances. Most of the periodic Requirements should have enough lag time built in to avoid the need for self-reporting in emergency situations. Otherwise, it is not envisioned all compliance activities should cease in a CIP Exceptional Circumstance, but only the ones indicated in the Requirements.

One commenter proposed revisions to the following initial periodic Requirements, and the SDT responds in order:

- CIP-004-5 Requirement Parts 4.2 through 4.4 should be required on or before the effective date to preclude record-keeping errors. The SDT notes that record-keeping errors, while not the most efficient, are not violations of the standard.
- CIP-006-5 Requirement Part 3.2 should tie to the previous testing interval and allow 24 months for the newly in-scope Cyber Assets. In response, tying the interval to previously in-scope Critical Cyber Assets would cause more confusion than is necessary for this Requirement, and the SDT believes the 12 calendar months are appropriate timeframes for testing PACS.
- CIP-008-5 Requirement Part 3.1 and CIP-009-5 Requirement Part 3.1 should not be included in the initial performance of periodic requirements section since they are not periodic, but are performed in response to a test. The SDT agrees.
- CIP-010-1 Requirement Parts 3.1 and 3.2 should not be included because it would be similar to part 3.3 in adding a new Cyber Asset to the BES Cyber System. In response, the SDT retains the additional timeframe because strict compliance would suggest this periodic timeframe be performed immediately on the effective dates for all BES Cyber Systems in scope, which would be infeasible for most all entities.
- CIP-009-5 Requirement Part 2.3 is included in both groups 6 and 7. The SDT notes this is not the case.

- Group 8 of the periodic Requirements dealing with the continued effectiveness of previous personnel risk assessments is already incorporated in the Requirement language. In response, strict compliance with the Requirement would otherwise suggest immediate compliance with this Requirement on the effective date.

One commenter suggested that NERC imposing Requirements before the effective date goes beyond NERC's legal authority. In response, the implementation plan does not modify the effective date of any Requirement but makes clear when the initial performance must occur for certain Requirements. By stating a Requirement can be performed prior to the effective date does not impose a different effective date. Rather, this clarifies that on the effective date, the entity has complied with the Requirement by performance of a past activity.

There was an observation that CIP-006-5 Requirement Part 3.1 and the Requirements specified in section 7 have periodicities longer than the initial performance. This is correct and intended by the SDT because even though the periodicity is longer, the benefit achieved by the initial performance puts it closer to the effective date.

Previous Identity Verification

One commenter noted an incorrect reference to CIP-004-5 Requirement Part 4.1, and the SDT expresses their gratitude for uncovering this error.

Planned or Unplanned Changes Resulting in a Higher Categorization

Several commenters suggested that the distinction between planned and unplanned changes is not clear and the timeframe for planned changes should be extended to 18-24 months. In response, the SDT carries forward this language that has been in effect since Version 2. The 12 months is also carried forward as the time entities with existing CCAs have to implement CIP Requirements on new CCAs. The SDT does not consider this 12 month timeframe unreasonable and notes in the example given that updates to a generation facility would be considered a planned change and compliance would be part of the maintenance performed during the outage.

One commenter stated that the addition of time for initial performance of periodic Requirements muddles the timeline for compliance. In response, the implementation plan would not preclude an entity from complying earlier to benefit the entity with a consistent compliance schedule, but without this provision, the periodic Requirements would need to be performed prior to the 12 month period, and this is neither reasonable nor appropriate. This language was added since the last posting in response to multiple entities' request.

There was a comment that suggested the last scenario in unplanned changes be clarified as the first high or medium impact BES Cyber System overall rather than at a facility. The SDT has made this clarification by providing a clarifying parenthetical phrase to row five of the "Scenario of Unplanned Changes After the Effective Date" table that underscores the meaning of that row in relation to and in context with rows one through four.

There was a request for clarification on the use of Effective Date in the table heading "Scenario of Unplanned Changes After the Effective Date". In response, the SDT notes that this is the effective date specified in each standard for Version 5 of the CIP Cyber Security Standards.

Applicability Reference Tables

One commenter proposed revisions to the Requirement applicability, and the SDT responds in order:

- CIP-004-5 Requirements R4 and R5 should apply to Protected Cyber Assets. In response, we have addressed most of the risk by authorizing and revoking access associated with the BES Cyber System. We carry forward the precedent of applicability in this case from previous standards, and do not find a justification for adding them to the applicability of these Requirement Parts.
- CIP-005-5 Requirement R1 should apply to PACS as it does in the current standard.
- CIP-005-5 R1 should apply to PACS as it does in the current standard. In previous versions, CIP-005 R2 applied but not R1. The SDT received significant industry feedback that this applicability was confusing and resulted in multiple interpretations. The SDT addresses access control at the device level in CIP-007-5 and avoids the confusion around the disconnect between applicability in CIP-005-4 R1 and R2, and for this reason, CIP-005-5, Requirement R1 does not apply to PACS.

There was a comment that CIP-005-5 Requirement R2 should apply to EACMS. In response, the EACMS are referenced as part of the Requirement. The confusion of recursive Requirements is not worth the reliability and security benefit gained by their inclusion.

Definitions

BES Cyber Asset

One entity commented that the definition should reference "the items in Attachment 1" instead of "Facilities, systems, or equipment," because "Facilities, systems, or equipment" is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. The SDT points out that a definition is used in a standard and cannot reference a part of the standard. The term "Facilities, systems or equipment" has been used as part of the definition of Critical Assets for Versions 1, 2, 3 and 4.

BES Cyber System

One commenter wrote that the definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped. The SDT believes that the rest of the definition of the BES Cyber System in relation to the performance of reliability functions provides clarity to the meaning used here.

BES Cyber System Information Responses

The SDT received a concern regarding the phrase "not publicly available" in that if BES Cyber System Information was made public, it would then be outside the scope of the standard. The SDT appreciates this concern; however, it believes that the meaning is ultimately clear as to the intent.

CIP Exceptional Circumstance Responses

The SDT received a request to clarify the punctuation in the definition of CIP Exceptional Circumstances. The SDT has updated the punctuation as requested.

One commenter expressed concern about the ability to declare a CIP Exceptional Circumstance for hardware, software or equipment failure. The concern of the commenter was that this could open the door to bypassing Requirements for minor issues. The SDT did not envision this as a free for all and believes that the obligation to have policy around the declaration and response to CIP Exceptional Circumstances should minimize any abuse of this definition.

CIP Senior Manager Responses

One commenter requested that the SDT address the accepted interpretation request in RFI Project 2012-INT-06. While the SDT has an obligation to incorporate existing interpretations, the response to the interpretation that was highlighted has not been posted and therefore the SDT would risk contradicting a pending standards interpretation action.

Additionally, since that interpretation has not been approved by industry, there is no way for the SDT to determine whether it reflects a level of consensus of the industry. As such, the SDT believes that this would be too large of a change to incorporate at this point in the development process.

Control Center

Many entities requested clarification on the term “associated data centers” in the definition of Control Centers and asked whether these are the "data centers" that service/support a control center”. Comments were also made that “data center” is not a defined term. The SDT believes that the term “data center” is a commonly understood term of practice and that a specific glossary definition is not required. The intent of including “associated data centers” in the definition of Control Centers is to include only those systems that are associated with the Control Center Cyber Assets and directly support the functions of the functional entities defined. These will be the BES Cyber Systems that directly provide monitoring and control functions for the Control Center operators’ use in the performance of their real-time functions, and to ensure that this does not include certain types of field data aggregating or processing assets that are associated with field transmission or generation assets. Control Center data centers do not necessarily reside in the same facility where operators are hosted, but may extend the Control Center to include facilities hosting these cyber systems outside of the facility hosting the Control Center operators.

One entity requested clarification on the meaning of “location” in the definition. The NERC Guideline for Critical Asset identification has an extensive discussion of control rooms and Control Centers. In general, a location is delineated by a physical boundary that hosts a set of BES Facilities.

One entity suggested the addition of “CIP” to the term or some indication that this is only a definition used in the CIP context. The SDT is proposing the term to be included in the NERC Glossary. The convention is that when the term is used in its capitalized form (initial letter of each word), then it is used as the NERC Glossary defined meaning of the term. Otherwise, it is used in the undefined, generic meaning. This does not have any effect on other standards that do not use the term in its capitalized form. Other standards which wish to use the NERC Glossary term as defined (or wish to amend it through the development process) can use the capitalized form.

Cyber Asset

One entity commented that the inclusion of “hardware, software and data” in the definition of Cyber Asset was redundant and proposed a simplified definition of “Entity programmable electronic devices”. The SDT’s approach to existing definitions is to make only the modifications necessary for additional clarity or intent. This definition is based on

the previous definition of Cyber Asset. The SDT believes that removing the terms "hardware, software and data" would not provide additional clarity and that the addition of "Entity" in the qualification of "programmable" would inappropriately limit the general scope of the definition of cyber asset. The protection Requirements in the standards include those necessary to ensure that proper processes are included for protection from inappropriate modification or misuse of programs not directly modified by the entity.

Another entity commented that the proposed definition could be interpreted to require utilities to demonstrate consideration of - in addition to hardware - all software and data on each programmable electronic device, which would be impracticable and overly burdensome. The entity recommends changing the definition to "Programmable electronic device." The SDT points out that the inclusion of these qualifications has been part of the definition of cyber assets since Versions 1, 2, 3 and 4 and that the modifications to the previous definition ensures that the definition includes the data when it is on these devices.

One entity commented that the inclusion in voice communication for a Control Center operator to implement operating actions in the execution of a Control Center functional obligation would include many smaller entities as Control Centers. The determination of whether a facility is considered a Control Center is dependent on whether it meets the definition, not on size or on how it performs its functional obligations. The manner in which it implements its functional obligations will determine what are qualified BES Cyber Assets. For example, in the environment that the commenter describes, there may be many BES Cyber Assets that provide monitoring and alarming information on which the operator will initiate a real-time operation for the BES. The impact of such monitoring and alarming systems on the real-time operation of the BES warrants the protection commensurate with its function.

Cyber Security Incident

One commenter suggested modifying the definition of Cyber Security Incident to eliminate attempts of compromise or disruption because such a definition is broad enough to include any erroneous traffic. The SDT disagrees. Attempts of compromise imply intent far beyond erroneous traffic and should be analyzed and recorded as part of the CIP-008-5 incident response plan.

There was a comment that the definition of Cyber Security Incident should also apply to PCAs, EACMS and PACS. In response, the definition has no applicability, and an incident occurring on PCAs, EACMS and PACS already meets the definition of having the potential to impact the BES Cyber System.

There was a comment suggesting that it is difficult to determine the intent of an attacker, and the commenter further suggested that "suspicious" is vague. In response, the SDT intends that such determination is best left to the entity. Without the qualifiers of suspicious and malicious, it could be interpreted that many nominal events would be considered Cyber Security Incidents.

Electronic Access Control and Monitoring System

One commenter stated that the definition of EACMS is inconsistent with the definition used in the background section of Version 5 CIP Standards. In response, the guidance provided in the background section is not a definition. It only provides example EACMS for the purpose of adding context for the reader.

Intermediate Device (now "Intermediate System")

A recommendation was made that the definition of Intermediate Device be modified to remove the phrase "or collection of Cyber Assets", as they consider this limiting the scope. The SDT used "A Cyber Asset or collection of Cyber Assets" to allow for flexibility so that an entity could use one or more devices to perform the noted functional Requirements. The scope of the definition and Requirements is limited to only Interactive Remote Access to BES Cyber Systems. Further, it was noted in prior comments that entities may not be able to implement a single device that provides encryption and multifactor authentication. As a result of comments, the definition has been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards.

One commenter requested clarification on the definition of Intermediate Device. The SDT has worked the definition to allow for flexibility in the selection and implementation of technology to meet their needs. The definition does not prevent an entity from having an Intermediate Device within an ESP, just not the ESP containing the BES Cyber Systems being remotely accessed. The definition term (not the definition's meaning) has also been modified to "Intermediate System" to better align with the asset and system concepts used throughout the Version 5 standards. Additional references are available in the *Guidance for Secure Interactive Remote Access* document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

One commenter requested more clarity regarding the types of devices that would qualify as intermediate devices, beyond the Requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Additional references are available in the *Guidance for Secure Interactive Remote*

Access document. There are case examples showing differing implementations. See http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

Interactive Remote Access

One commenter suggested that, as written, the definition appears to require that entities declare each of their internal networks as an ESP, including their corporate networks. The commenter discussed that many entities monitor their corporate network in much the same manner as their ESPs, and that requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. The commenter requested appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only. In response, the SDT notes that it is not necessary to declare the encryption termination point as a part of the ESP. It is allowable to have the termination point reside outside of the ESP, such as a corporate firewall to allow for corporate boundary systems to monitor network traffic as described. In this scenario, the corporate firewall would be considered and protected as an EACMS but still not considered to define an ESP.

There was a recommendation to remove the second sentence of the Interactive Remote Access definition. The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

One comment suggested that the definition of Interactive Remote Access be modified to remove the sentence, "Remote access can be initiated from: ... contractors and consultants." The SDT added this language to address comments and concerns raised during this project and Project 2010-15: Expedited Revisions to CIP-005-3.

There was one request that the definition be modified as "access is likely initiated…" The SDT used "may be initiated" to allow for flexibility rather than using words such as "shall be initiated" or "will be initiated" which are far more restrictive and align to the concern noted.

There was a suggestion that the definition of Interactive Remote Access be modified to remove Requirement language within the definition. The SDT considers all parts of the definition to be clarification of what is and is not Interactive Remote Access. The Requirements are the technical controls to be implemented.

Reportable Cyber Security Incident

There was a comment suggesting that the definition of Reportable Cyber Security Incident is too broad and should specifically state that a malware infection of an in-scope Cyber Asset should be reported. In response, the SDT provides additional guidance in the context of CIP-008-5 that would generally ensure the proper reporting of a malware infection. However, a malware infection itself would cause additional uncertainty in the definition. Moreover, entities would be left to wonder if a contained malware infection was reportable or not. For these reasons, the SDT does not agree with the recommendation to further specify Reportable Cyber Security Incident.

One commenter said that this definition should be removed and addressed solely within the standard. In response, the SDT believes there is sufficient consensus for the definition and moving this term to a local definition in CIP-008-5 would be a significant change and potentially cause uncertainty in the enforceability of this definition.

Exhibit E

1.) Table of VRFs and VSLs Proposed for Approval
2.) Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines

Exhibit E

1.) Table of VRFs and VSLs Proposed for Approval

Project 2008-06 - Cyber Security Order No. 706 - V5

Consolidated VSLs from all standards

October 26, 2012

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	High	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized	four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of	six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or	to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified;	medium impact and BES Cyber Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible	or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or medium BES Cyber Systems have not been identified.	Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	
R2	**Operations Planning**	**Lower**	The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications

R #	Time Horizon	VRF	Violation Severity Levels (CIP-002-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months of the previous approval. (R2.2)	approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the previous approval. (R2.2)	required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 15 calendar months but did complete this	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 16 calendar	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did	within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar	documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	
R2	**Operations Planning**	**Lower**	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2)	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this	Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this	OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R2)	review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of	review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				the previous approval. (R2)	the previous approval. (R2)	
R3	**Operations Planning**	**Medium**	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)
R4	**Operations Planning**	**Lower**	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 30	The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, and	The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, but does not have a process to delegate actions from the CIP Senior Manager. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			calendar days but did document this change in less than 40 calendar days of the change. (R4)	delegate within 40 calendar days but did document this change in less than 50 calendar days of the change. (R4)	has Identified deficiencies but did not assess or correct the deficiencies.(R4) OR The Responsible Entity has used delegated authority for actions where allowed by the CIP Standards, has a process to delegate actions from the CIP Senior Manager, but did not identify, assess, or correct the deficiencies.(R4) OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions	OR The Responsible Entity has identified a delegate by name, title, date of delegation, and specific actions delegated, but did not document changes to the delegate within 60 calendar days of the change. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-003-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					delegated, but did not document changes to the delegate within 50 calendar days but did document this change in less than 60 calendar days of the change. (R4)	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Lower**	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)
R2	**Operations Planning**	**Lower**	The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals	and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals	The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)
R3	**Operations Planning**	**Medium**	The Responsible Entity has a program for	The Responsible Entity has a program for conducting Personnel	The Responsible Entity has a program for conducting Personnel	The Responsible Entity did not have all of the required elements as

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess,	described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including	correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors,	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess,	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess,	including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted	and correct the deficiencies. (3.5)	and correct the deficiencies. (3.5)	for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)			
R4	**Operations Planning and Same Day Operations**	**Lower**	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not identify, assess and	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2)	The Responsible Entity did not implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies.	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for	storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			(4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						for four or more BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)
R5	**Same Day Operations and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1)	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1)	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or	access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR	more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct			

R #	Time Horizon	VRF	Violation Severity Levels (CIP-004-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			the deficiencies. (5.5)			

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-5 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning** **Same-Day Operations**	**Medium**	The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies.	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	(1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to	operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					monitor for unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	deficiencies, but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						(1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and identified deficiencies, but did not assess or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical access logs for 90 calendar days. (1.9)
R2	**Same-Day**	**Medium**	N/A	The Responsible Entity	The Responsible Entity	The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Operations			included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or	included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		retain visitor logs for at least ninety days. (2.3)
R3	**Long Term Planning**	**Lower**	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity has documented and	The Responsible Entity has not documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar

R #	Time Horizon	VRF	Violation Severity Levels (CIP-006-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						months. (3.1)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Same Day Operations**	**Medium**	N/A	The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against	The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible,	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	
R2	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified and	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65	more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the	calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the	CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)		deficiencies. (2.4)
R3	**Same Day Operations**	**Medium**		The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR The Responsible Entity	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified deficiencies but did	more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)
R4	**Same Day Operations and Operations Assessment**	**Medium**	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4*

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system	and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did not assess or correct	detect and log all of the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	
R5	**Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that included the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the	identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the	the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System	applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			deficiencies. (5.6)	deficiencies. (5.6)	Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3)	process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only	OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within	procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal	deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold

R #	Time Horizon	VRF	Violation Severity Levels (CIP-007-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security Incident. (1.2)
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable	The Responsible Entity has not tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					Cyber Security Incident occurs. (2.2)	
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities,	response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-008-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				or • Cyber Security Incident response groups or individuals, or • Technology changes.	or individuals, or • Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**Medium**	N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R2	**Operations Planning** **Real-time Operations**	**Lower**	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17 calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests,	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)
R3	**Operations Assessment**	**Lower**	The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the update being completed. (3.1.3)	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each recovery plan test or actual recovery. (3.1.1)	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of each recovery plan test or actual recovery. (3.1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or	OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-009-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				• Responders, or • Technology changes.	responsibilities, or • Responders, or Technology changes.	

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline	identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required	correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline	management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the	configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s)	OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
				existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to verify that required	process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did	not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an	the test and production environments. (1.5.2)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments and identified deficiencies but did not assess or correct the	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1)	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	N/A		The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-011-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	
R2	**Operations Planning**	**Lower**	N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

Exhibit E

2.) Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines

Project 2008-06 - Cyber Security - Order 706 - V5

These tables provide analysis and justification for each VRF and VSL for each requirement in the Version 5 CIP Cyber Security Standards:

VRF and VSL Justifications – CIP-002-5, R1	
Proposed VRF	**HIGH**
NERC VRF Discussion	A VRF of High is assigned to this Requirement. The requirement specifies the "bright-line" criteria used to categorize Bulk Electric System (BES) Cyber Systems, and the identification of High and Medium impact BES Cyber Systems. A VRF assignment of High is consistent with the higher risk impact of a violation of the identification and categorization of High and Medium impact BES Cyber Systems, as well as the failure to identify and appropriately re-categorize the affected BES Cyber Systems after a BES reconfiguration. The compromise of these Systems due to a cyber security incident could lead to significant impact, up to and including cascading disturbances. Failure to protect High and Medium impact Cyber Assets and their potential compromise may cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. The impact categorization of BES Cyber Systems is based on their impact on the reliable operation of the BES. The criteria are based on BES functional tasks that map to the areas cited in the Blackout Report.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The Requirement specifies the "bright-line" criteria used to categorize Bulk Electric System (BES) Systems and the identification of High and Medium impact BES Cyber Systems. The VRF is only applied at the requirement level and the requirement part is treated equally. A VRF assignment of High is consistent with the higher risk impact of a violation of the identification and categorization of High and Medium impact BES Cyber Systems, as well as the failure to identify and appropriately re-categorize the affected

VRF and VSL Justifications – CIP-002-5, R1			
	BES Cyber Systems after a BES reconfiguration. The compromise of these Systems due to a cyber security incident could lead to significant impact, up to and including cascading disturbances.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-002-3/4, R2, which has an approved VRF of High and the proposed VRF for CIP-002-5, R1 remains consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to protect High and Medium impact Cyber Assets and their potential compromise may cause or contribute to Bulk Electric System instability, separation, or a cascading sequence of failures, or could place the Bulk Electric System at an unacceptable risk of instability, separation, or cascading failures. Therefore, this requirement was assigned a High VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-002-5-2, Requirement R1 contains one main objective: The identification and categorization of High and Medium impact BES Cyber Systems for the application of specific protective cyber security requirements and the application of programmatic controls to Low impact BES Cyber Systems. Since the requirement focuses on the specific identification and categorization of such High and Medium impact Systems, an assignment of a High VRF is justified.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
For Responsible Entities with more than a total of 40 BES assets in Requirement R1, five percent or fewer BES assets have not been considered according to Requirement R1;	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than five percent but less than or equal to 10 percent of BES assets have not been	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 10 percent but less than or equal to 15 percent of BES assets have not been considered, according to	For Responsible Entities with more than a total of 40 BES assets in Requirement R1, more than 15 percent of BES assets have not been considered, according to Requirement R1;

VRF and VSL Justifications – CIP-002-5, R1			
OR For Responsible Entities with a total of 40 or fewer BES assets, 2 or fewer BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer identified BES Cyber Systems have not been categorized or have been incorrectly	considered, according to Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than two, but fewer than or equal to four BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a	Requirement R1; OR For Responsible Entities with a total of 40 or fewer BES assets, more than four, but fewer than or equal to six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high or medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high or medium impact and BES Cyber	OR For Responsible Entities with a total of 40 or fewer BES assets, more than six BES assets in Requirement R1, have not been considered according to Requirement R1; OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower

VRF and VSL Justifications – CIP-002-5, R1			
categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, five percent or fewer high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, five or fewer high or medium BES Cyber Systems have not been identified.	total of 100 or fewer high and medium impact and BES Cyber Systems, more than five but less than or equal to 10 identified BES Cyber Systems have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than five percent but less than or equal to 10 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than five but less than or equal to 10 high or	Assets, more than 10 but less than or equal to 15 identified BES Cyber Assets have not been categorized or have been incorrectly categorized at a lower category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 10 percent but less than or equal to 15 percent high or medium BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 10 but less than or equal to 15 high or medium BES Cyber Systems have not been identified.	category. OR For Responsible Entities with more than a total of 100 high and medium impact BES Cyber Systems, more than 15 percent of high or medium impact BES Cyber Systems have not been identified; OR For Responsible Entities with a total of 100 or fewer high and medium impact BES Cyber Systems, more than 15 high or medium impact BES Cyber Systems have not been identified.

VRF and VSL Justifications – CIP-002-5, R1			
	medium BES Cyber Systems have not been identified.		

VRF and VSL Justifications – CIP-002-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has correctly categorized their BES Cyber Systems but fails to identify or correctly categorize one or more of them. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The paradigm in CIP-002-5 has evolved from a binary model to a multidimensional model that includes identification and categorization. The VSLs provided reflect this paradigm and is fundamentally different from the binary model in CIP Versions 1 to 4. With this fundamental difference, the VSLs are not intended to lower the current reliability objective sought by this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs do not use any ambiguous terminology; thereby, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-002-5, R1	
Ambiguous Language	

VRF and VSL Justifications – CIP-002-5, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	This requirement is an identification and categorization requirement and a single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and	Not applicable since this requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-002-5, R1	
implementation should account for their interdependence	

VRF and VSL Justifications – CIP-002-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. The requirement specifies an annual review and approval of the identification and categorization of BES Cyber Systems. The impact of a failure to review and approve the identification and categorization within the prescribed period has minimal impact on the reliability and operability of the BES. The requirement is a requirement that, if violated, would not be expected to directly or adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. The requirement has no bearing on the areas cited in the Blackout Report.
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement has no subpart, and its assignment of a Lower VRF is consistent with the impact of a violation of this requirement. The impact of a failure to review and approve the identification and categorization within the prescribed period has minimal impact on the reliability and operability of the BES. The requirement is administrative in nature and is a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps to CIP-002-4 R3, which has an assigned VRF of Lower and the proposed VRF for CIP-002-5, R2, remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-002-5, Requirement R2 requires an annual review and approval. The requirement is a requirement

VRF and VSL Justifications – CIP-002-5, R2			
	that, if violated, would not be expected to directly adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. Therefore, this requirement was assigned a Lower VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-002-5, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not complete its review and update for the identification required for R1 within 15 calendar months but less than or equal to 16 calendar months of the previous review. (R2.1) OR The Responsible Entity did not complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity did not complete its review and update for the identification required for R1 within 16 calendar months but less than or equal to 17 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity did not complete its review and update for the identification required for R1 within 17 calendar months but less than or equal to 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 17 calendar months but less than or equal to 18 calendar months of the	The Responsible Entity did not complete its review and update for the identification required for R1 within 18 calendar months of the previous review. (R2.1) OR The Responsible Entity failed to complete its approval of the identifications required by R1 by the CIP Senior Manager or delegate according to Requirement R2 within 18 calendar months of the previous approval. (R2.2)

VRF and VSL Justifications – CIP-002-5, R2			
of the previous approval. (R2.2)	of the previous approval. (R2.2)	previous approval. (R2.2)	

VRF and VSL Justifications – CIP-002-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has appropriately reviewed and updated their identification of BES Cyber Systems but failed to complete the review and update within the specified timeframes. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed requirement is mapped to requirement R3 of CIP-002-3. The VSLs for the previous releases were based on lists of Critical Assets and Critical Cyber Assets, with separate requirements for review and approval. This version requires identification and categorization of BES Cyber Systems within a prescribed period. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-002-5, R2	
Ambiguous Language	

VRF and VSL Justifications – CIP-002-5, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement; and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	This requirement is a periodic review and approval requirement and does not specify protective requirements.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and	Not applicable since this requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-002-5, R2	
implementation should account for their interdependence	

VRF and VSL Justifications – CIP-003-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium was assigned to this requirement. Security policies enable effective implementation of the CIP standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. Periodic review and approval of the cyber security policy ensures that the policy is kept up-to-date and periodically reaffirms management's commitment to the protection of its BES Cyber Systems. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. Failure to provide clear governance may lead to ineffective controls, which could compromise security; and, therefore, the integrity of the Bulk Electric System. Consequently, a VRF of Medium was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level, and the requirement parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Medium is consistent with the risk impact of a violation across the entire requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R1, which has an approved VRF of Medium; therefore, the proposed VRF remains consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy is unlikely, under Emergency, abnormal, or

VRF and VSL Justifications – CIP-003-5, R1			
	restoration conditions anticipated by the preparations to lead to Bulk Electric System instability, separation, or cascading failures, nor to hinder restoration to a normal condition. Therefore, this requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address one of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address two of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address three of the nine topics required by R1. (R1) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 within 17 calendar months but did complete	The Responsible Entity documented and implemented one or more cyber security policies for its high impact and medium impact BES Cyber Systems, but did not address four or more of the nine topics required by R1. (R1) OR The Responsible Entity did not have any documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1. (R1)

VRF and VSL Justifications – CIP-003-5, R1			
R1 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 15 calendar months but did complete this approval in less than or equal to 16 calendar months of the previous approval. (R1)	R1 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous approval. (R1)	this review in less than or equal to 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R1)	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies as required by R1 within 18 calendar months of the previous review. (R1) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for its high impact and medium impact BES Cyber Systems as required by R1 by the CIP Senior Manager or delegate according to Requirement R1 within 18 calendar months of the previous approval. (R1)

VRF and VSL Justifications – CIP-003-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement, and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to previously approved requirements CIP-003-3 R1 and CIP-003-3 R1.2. The VSLs were combined for these requirements using a gradated methodology. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement; and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and,

VRF and VSL Justifications – CIP-003-5, R1	
documentation and implementation should account for their interdependence	therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower was assigned to this requirement. Security policies enable effective implementation of the CIP standard's requirements. The purpose of policies is to provide a management and governance foundation for all requirements that apply to personnel who have authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems. People are a fundamental component of any security program. Consequently, proper governance must be established in order to provide some assurance of organizational behavior. However, given the scoping of the this requirement to only those BES assets that contain low impact BES Cyber Systems, a VRF of Lower was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for the Responsible Entity to implement a documented cyber security policy that contains certain elements specified in the requirement. The VRF is only applied at the requirement level and the Requirement Parts are treated in aggregate. While the requirement specifies a number of elements, not necessarily parts, that must be included in the cyber security policy, the VRF is reflective of the policy as a whole. Therefore, the assigned VRF of Lower is consistent with the risk impact of a violation across the entire requirement for BES assets that contain low impact BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R1, which has an approved VRF of Lower but applies to Cyber Assets with an inherently lower risk; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to properly implement the cyber security policy would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.

VRF and VSL Justifications – CIP-003-5, R2			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The cyber security policy requirement encompasses a number of policy domains. The VRF is identified at the risk level represented by all of the policy domains in aggregate. Therefore, the VRF is consistent with the highest risk reliability objective contained in the requirement.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only three of the topics as required by R2 but did not identify, assess, or correct the	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only two of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity documented and implemented one or more cyber security policies for assets with a low impact rating that address only one of the topics as required by R2 but did not identify, assess, or correct the deficiencies.	The Responsible Entity did not document or implement any cyber security policies for assets with a low impact rating that address the topics as required by R2. (R2) OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber

VRF and VSL Justifications – CIP-003-5, R2			
deficiencies. OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 15 calendar months but did complete this review in less than or equal to 16 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 15 calendar months but did complete this approval in less than or equal to 16 calendar	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 16 calendar months but did complete this review in less than or equal to 17 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 16 calendar months but did complete this approval in less than or equal to 17 calendar months of the previous	OR The Responsible Entity did not complete its review of the one or more documented cyber security policies for assets with a low impact rating as required by R2 within 17 calendar months but did complete this review in less than or equal to 18 calendar months of the previous review. (R2) OR The Responsible Entity did not complete its approval of the one or more documented cyber security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 17 calendar months but did complete this approval in less than or equal to 18 calendar months of the previous approval. (R2)	security policies for assets with a low impact rating as required by R2 by the CIP Senior Manager according to Requirement R2 within 18 calendar months of the previous approval. (R2)

VRF and VSL Justifications – CIP-003-5, R2			
months of the previous approval. (R2)	approval. (R2)		

VRF and VSL Justifications – CIP-003-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to previously approved requirements CIP-003-3 R1 and CIP-003-3 R1.2. The VSLs were combined for these requirements using a gradated methodology. The proposed VSLs do not have the unintended consequence of lowering the level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The Proposed VSLs are not binary and does not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this requirement in that some measurable reliability benefit can be achieved if the Responsible Entity has documented cyber security policies but fails to address one or more of the required topics. A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case; as such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and, therefore,

VRF and VSL Justifications – CIP-003-5, R2	
documentation and implementation should account for their interdependence	accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-003-5, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The identification of a single CIP Senior Manager ensures that there is clear authority and ownership for the CIP program within an organization. Cyber security is not simply a technical endeavor. Failure to provide clear governance and organizational leadership may lead to ineffective controls, which could compromise security and, therefore, the integrity of the Bulk Electric System. Consequently, a VRF of Medium was selected.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement specifies that a CIP Senior Manager be identified. The VRF is only applied at the requirement level and the requirement parts are treated equally. As there are no requirement parts, the VRF is, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-003-3, R2, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Because the purpose of the Requirement is for entities to properly identify and document the CIP Senior Manager in order to ensure there is clear authority and ownership of the CIP program within an organization, this Requirement is appropriately assigned a Medium VRF.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement does not co-mingle more than one obligation. The only obligation included in requirement CIP-003-5 R1 is the identification of the CIP Senior Manager. Therefore, the requirement has a single VRF.

VRF and VSL Justifications – CIP-003-5, R3			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 30 calendar days but did document this change in less than 40 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 40 calendar days but did document this change in less than 50 calendar days of the change. (R3)	The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 50 calendar days but did document this change in less than 60 calendar days of the change. (R3)	The Responsible Entity has not identified, by name, a CIP Senior Manager. OR The Responsible Entity has identified by name a CIP Senior Manager, but did not document changes to the CIP Senior Manager within 60 calendar days of the change. (R3)

VRF and VSL Justifications – CIP-003-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity identified its CIP Senior Manager but failed to document changes within the specified timeframes. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement, CIP-003-5 R3, maps to a previously approved requirement, CIP-003-3 R2. The proposed VSLs do not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-003-5, R3	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	There is an incremental aspect to a violation of this Requirement in that some measurable reliability benefit can be achieved if the Responsible Entity identified its CIP Senior Manager but failed to document changes within the specified timeframes.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	Not applicable since the requirement does not contain interdependent tasks of documentation and implementation.

VRF and VSL Justifications – CIP-003-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-003-5, R4	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability purpose of this requirement is to ensure clear lines of authority and ownership for security matters that could impact the stability and integrity of the Bulk Electric System, that delegations are kept up-to-date, and that individuals do not assume undocumented authority. As this requirement is only a part of the overall governance structure of a cyber security program, which includes additional leadership and policy, a VRF of Lower was assigned to this requirement.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement directs that the CIP Senior Manager is responsible for all approval and authorizations, but also grants the CIP Senior Manager with the ability to delegate this authority. The Requirement also calls for changes to the CIP Senior Manager and any delegations to be documented within 30 calendar days. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The requirement does not contain parts and are, therefore, consistent.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-003-3, R 2.2 and R2.3, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to show clear authorization for actions taken back to the CIP Senior Manager would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The obligation of this requirement is to demonstrate that the CIP Senior Manager is ultimately responsible for all approvals and authorizations required in the CIP Standards. This requirement allows for delegation,

VRF and VSL Justifications – CIP-003-5, R4			
	but also obligates the Responsible Entity to document these delegations. The VRF was chosen based upon the highest reliability risk objective, which is the clear line of authority to the CIP Senior Manager and are, therefore, consistent with VRF Guideline 5.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity failed to document the approval and authorization of one delegation (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of two delegations (by title or name of the delegate) as required.	The Responsible Entity failed to document the approval and authorization of three or more delegations (by title or name of the delegate) as required.

VRF and VSL Justifications – CIP-003-5, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to the violation, and the VSLs follow the guidelines for incremental violations. There is a single element upon which severity may be gradated; as such, gradated VSLs were assigned.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps back to a previously approved VSL in CIP-003-3 R2.2 and R2.3. The previously approved VSL was a binary Severe VSL. The SDT has determined that there are numerous delegations that take place, and there is a reliability benefit if the majority of those delegations are documented in compliance with the standard; and, as such, has assigned gradated VSLs to the requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore,

VRF and VSL Justifications – CIP-003-5, R4	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The requirement contains interdependent tasks of documentation and implementation. The VSL requirement presumes that the only way to demonstrate compliance is through documentation; as such, The VSLs are based upon the documentation measure, and implementation is assumed with documentation, therefore accounting for the interdependence in these tasks.

VRF and VSL Justifications – CIP-004-5, R1	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have awareness of sound security practices. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for ongoing security awareness reinforcement. The VRF is only applied at the Requirement level and the requirement parts are treated equally. The single Requirement Part constitutes the required security awareness program.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-3, R1, which has an approved VRF of Lower; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to convey security awareness practices within a calendar quarter would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring individuals with access to BES Cyber Systems have awareness of sound security practices and, therefore, does not co-mingle more than one obligation.

VRF and VSL Justifications – CIP-004-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter. (1.1)	The Responsible Entity did not reinforce cyber security practices during a calendar quarter but did so within the subsequent quarter but beyond 30 calendar days after the start of that calendar quarter. (1.1)	The Responsible Entity did not document or implement any security awareness process(es) to reinforce cyber security practices. (R1) OR The Responsible Entity did not reinforce cyber security practices and associated physical security practices for at least two consecutive calendar quarters. (1.1)

VRF and VSL Justifications – CIP-004-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines —There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. The SDT has determined that there is a reliability benefit to partial compliance with this requirement and has therefore assigned gradated VSLs.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R1, which did not graduate VSLs according to the time beyond meeting a compliance obligation and accumulated violations as a single violation. This version corrects the oversight by gradating the violation based on the number of days past the performance requirement. Failure to meet the requirement by a given number of days appropriately maps to the severity of the violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore,

VRF and VSL Justifications – CIP-004-5, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-5, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective would not have adverse effect on the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-004-3, R2.2, which has an approved VRF of Medium. In this version, the training program requirements are distinct from the implementation, and the implementation in R3 has the previously approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a training program would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.

VRF and VSL Justifications – CIP-004-5, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented a cyber security training program but failed to include one of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train one individual (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct	The Responsible Entity implemented a cyber security training program but failed to include two of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train two individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR	The Responsible Entity implemented a cyber security training program but failed to include three of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals (with the exception of CIP Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train three individuals with	The Responsible Entity did not implement a cyber security training program appropriate to individual roles, functions, or responsibilities. (R2) OR The Responsible Entity implemented a cyber security training program but failed to include four or more of the training content topics in Requirement Parts 2.1.1 through 2.1.9, and did not identify, assess and correct the deficiencies. (2.1) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals (with the exception of CIP

VRF and VSL Justifications – CIP-004-5, R2			
the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train one individual with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	The Responsible Entity implemented a cyber security training program but failed to train two individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)	Exceptional Circumstances) prior to their being granted authorized electronic and authorized unescorted physical access, and did not identify, assess and correct the deficiencies. (2.2) OR The Responsible Entity implemented a cyber security training program but failed to train four or more individuals with authorized electronic or authorized unescorted physical access within 15 calendar months of the previous training completion date, and did not identify, assess and correct the deficiencies. (2.3)

VRF and VSL Justifications – CIP-004-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The requirement maps to CIP-004-3 R2.2, which did not graduate VSLs and treats all violations equally. This version corrects the oversight by gradating the violation based on the number of training elements missing in the program. Failure to meet the parts of the requirement appropriately maps to the severity of the violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R2	
Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security.

VRF and VSL Justifications – CIP-004-5, R2	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	This VSL accounts for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation.

VRF and VSL Justifications – CIP-004-5, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role. Failure to meet this objective could affect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for implementing a training program for individuals needing or having access to the BES Cyber System. The VRF is only applied at the Requirement level and the requirement parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards.

VRF and VSL Justifications – CIP-004-5, R3			
	This requirement maps from CIP-004-3, R2, which has an approved VRF of Medium.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a security training program could effect the electrical state or capability of the Bulk Electric System. However, it is unlikely to lead to instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that individuals with access to BES Cyber Systems have training in subjects related to the security of the BES Cyber System and appropriate to their role and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for one individual, and did not identify, assess, and correct the deficiencies. (R3) OR	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for two individuals, and did not identify, assess, and correct the deficiencies. (R3) OR	The Responsible Entity has a program for conducting Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for three individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	The Responsible Entity did not have all of the required elements as described by 3.1 through 3.4 included within documented program(s) for implementing Personnel Risk Assessments (PRAs), for individuals, including contractors and service vendors, for obtaining and retaining authorized cyber or authorized unescorted physical access. (R3) OR The Responsible Entity has a program for conducting Personnel

VRF and VSL Justifications – CIP-004-5, R3			
The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for one individual, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for one individual, and did not identify, assess, and correct	The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for two individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for two individuals, and did not identify, assess, and	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for three individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for three individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs)	Risk Assessments (PRAs) for individuals, including contractors and service vendors, but did not conduct the PRA as a condition of granting authorized electronic or authorized unescorted physical access for four or more individuals, and did not identify, assess, and correct the deficiencies. (R3) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not confirm identity for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.1 & 3.4) OR

VRF and VSL Justifications – CIP-004-5, R3			
the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for one individual, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for one individual with authorized electronic or authorized unescorted physical access within 7 calendar years of the	correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for two individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for two individuals with authorized electronic or authorized unescorted physical access	for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for three individuals, and did not identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for three individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	The Responsible Entity has a process to perform seven-year criminal history record checks for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not include the required checks described in 3.2.1 and 3.2.2 for four or more individuals, and did not identify, assess, and correct the deficiencies. (3.2 & 3.4) OR The Responsible Entity did conduct Personnel Risk Assessments (PRAs) for individuals, including contractors and service vendors, with authorized electronic or authorized unescorted physical access but did not evaluate criminal history records check for access authorization for four or more individuals, and did not

VRF and VSL Justifications – CIP-004-5, R3			
previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)	within 7 calendar years of the previous PRA completion date, and did not identify, assess, and correct the deficiencies. (3.5)		identify, assess, and correct the deficiencies. (3.3 & 3.4) OR The Responsible Entity did not conduct Personnel Risk Assessments (PRAs) for four or more individuals with authorized electronic or authorized unescorted physical access within 7 calendar years of the previous PRA completion date and has identified deficiencies, and did not identify, assess, and correct the deficiencies. (3.5)

VRF and VSL Justifications – CIP-004-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R2.2, which did not gradate VSLs and treats all violations equally. This version more appropriately gradates the violation based on the number of individuals with access to BES Cyber Systems who did not receive training. Failure for a given number of individuals to receive training appropriately maps to the severity of the violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R3	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations. The requirement is to implement a training program and failure for a single individual to have training does not necessarily imply a single violation. An overall view of the training program must consider the number of individuals who failed to receive training for a given period.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single failure of this requirement does not compromise network computer security. Although failure to implement a training program could associatively affect the ways in which computer network security applies, it does not, by itself, indicate a failure of computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This Requirement pertains to implementing the cyber security program and does not require procedural documentation.

VRF and VSL Justifications – CIP-004-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-004-5, R4			
Proposed VRF	**LOWER**		
NERC VRF Discussion	The reliability objective is to ensure that individuals with access to BES Cyber Systems have received a personnel risk assessment. Failure to meet this objective could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for a personnel risk assessment program for individuals needing or having access to a BES Cyber System. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a personnel risk assessment program could have adverse effect on the electrical state or capability of the Bulk Electric System, but it is not expected to cause Bulk Electric System instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that documentation a personnel risk assessment is developed for individuals with access to BES Cyber Systems and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity did not	The Responsible Entity did not	The Responsible Entity did not	The Responsible Entity did not

VRF and VSL Justifications – CIP-004-5, R4			
verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so less than 10 calendar days after the start of a subsequent calendar quarter, and did not identify, assess and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.3)	verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for two BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the	verify that individuals with active electronic or active unescorted physical access have authorization records during a calendar quarter but did so between 10 and 30 calendar days after the start of a subsequent calendar quarter, and did not identify, assess, and correct the deficiencies. (4.2) OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for three BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR	implement any documented program(s) for access management. (R4) OR The Responsible Entity has implemented one or more documented program(s) for access management that includes a process to authorize electronic access, unescorted physical access, or access to the designated storage locations where BES Cyber System Information is located, and did not identify, assess, and correct the deficiencies. (4.1) OR The Responsible Entity did not verify that individuals with active electronic or active unescorted physical access have authorization records for at least two consecutive calendar quarters, and did not identify, assess, and correct the deficiencies. (4.2)

VRF and VSL Justifications – CIP-004-5, R4			
OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for one BES Cyber System Information storage location, privileges were incorrect or unnecessary, and did not identify, assess and correct the deficiencies. (4.4)	deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for two BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for three BES Cyber System Information storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)	OR The Responsible Entity has implemented processes to verify that user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber Systems, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.3) OR The Responsible Entity has implemented processes to verify that access to the designated storage locations for BES Cyber System Information is correct and necessary within 15 calendar months of the previous verification but for four or more BES Cyber System Information

VRF and VSL Justifications – CIP-004-5, R4			
			storage locations, privileges were incorrect or unnecessary, and did not identify, assess, and correct the deficiencies. (4.4)

VRF and VSL Justifications – CIP-004-5, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R3, which gradates the VSLs based on implementation of the Requirement. This does not lower the current level of compliance because new components of the program have been added.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R4	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required documented program(s) has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-004-5, R4	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-004-5, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures prompt revocation of access for individuals no longer needing access to BES Cyber Systems and BES Cyber System Information. Failure to revoke access to BES Cyber Systems and BES Cyber System Information within the required time frame is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to revoke access to BES Cyber Systems and BES Cyber System Information when individuals no longer need access. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. Each Requirement row contributes to the objective of this Requirement.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-004-3 R4.2, which has an approved VRF of Lower, and CIP-007-3 R5.2.3., which has an approved VRF of Medium. The Requirement only addresses the securing of shared accounts for termination in CIP-007-3 R5.2.3, and not the audit trail. Because the securing of shared accounts upon termination is consistent with CIP-004-3 R4.2, then we can imply a VRF of lower for that component of the Requirement. Therefore, the proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to revoke access to BES Cyber Systems and BES Cyber System Information may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this Requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Requirement R5 requires prompt revocation of access for individuals no longer needing access to BES

VRF and VSL Justifications – CIP-004-5, R5			
	Cyber Systems and BES Cyber System Information. Each part of Requirement R5 specifies the obligations to revoke access in various situations when an individual no longer needs such access.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for one individual, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's user accounts upon termination action but did not	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for one individual, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but,	The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for two individuals, and did not identify, assess, and correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for two individuals, did not revoke the	The Responsible Entity has not implemented any documented program(s) for access revocation for electronic access, unescorted physical access, or BES Cyber System Information storage locations. (R5) OR The Responsible Entity has implemented one or more process(es) to remove the ability for unescorted physical access and Interactive Remote Access upon a termination action or complete the removal within 24 hours of the termination action but did not initiate those removals for three or more individuals, and did not identify, assess, and correct the deficiencies. (5.1)

VRF and VSL Justifications – CIP-004-5, R5			
do so for within 30 calendar days of the date of termination action for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more process(es) to change passwords for shared accounts known to the user upon termination action, reassignment, or transfer, but did not do so for within 30 calendar days of the date of termination action, reassignment, or transfer for one or more individuals, and did not identify, assess, and correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more	for one individual, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for two individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more process(es) to revoke the individual's access to the designated storage locations for BES Cyber System Information but, for three or more individuals, did not do so by the end of the next calendar day following the effective date and time of the termination action, and did not identify, assess, and correct the deficiencies. (5.3)	OR The Responsible Entity has implemented one or more process(es) to determine that an individual no longer requires retention of access following reassignments or transfers but, for three or more individuals, did not revoke the authorized electronic access to individual accounts and authorized unescorted physical access by the end of the next calendar day following the predetermined date, and did not identify, assess, and correct the deficiencies. (5.2)

VRF and VSL Justifications – CIP-004-5, R5			
process(es) to determine and document extenuating operating circumstances following a termination action, reassignment, or transfer, but did not change one or more passwords for shared accounts known to the user within 10 calendar days following the end of the extenuating operating circumstances, and did not identify, assess, and correct the deficiencies. (5.5)			

VRF and VSL Justifications – CIP-004-5, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL gradates the severity based on whether the violation includes a scenario whether the individual no longer needed access, when an individual was terminated for cause, or when both occurred. The requirement no longer differentiates on scenarios of termination for cause.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-004-5, R5	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to implement programs for access revocation has a binary Severe VSL. A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-004-5, R5	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-005-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requirement ensures that all BES Cyber Systems are within an Electronic Security Perimeter and that all electronic routable communication and dialup communication across the perimeter is secured. Failure to properly secure the external communications to the BES Cyber Systems and the networks on which they reside could result in unauthorized access, which could directly affect the ability to control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Both Requirements in CIP-005 are of the same VRF as both insure the proper electronic security perimeter based controls are in place for preventing unauthorized access.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement's VRF is consistent with similar security requirements with similar risks in the other CIP standards.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement documented processes and adequate safeguards to prevent unauthorized access to an entity's networks could result in unauthorized access and potential disruption of monitoring and logical control of BES Cyber Assets. Consistent with the definition of a Medium VRF, unauthorized logical access could directly affect the electrical state or the capability of the Bulk Electric System and the ability to monitor and control the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common set of objectives to ensure access to BES Cyber Systems is authorized and protected. The obligations within the requirement collectively address the objective and only one VRF is assigned.

VRF and VSL Justifications – CIP-005-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for CIP-005-5 Table R1 – Electronic Security Perimeter. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

VRF and VSL Justifications – CIP-005-5, R1			
			OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)

VRF and VSL Justifications – CIP-005-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL's are in line with the currently approved VSL's in CIP-005-3a and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-005-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	With the exception of the portion of the VSLs dealing with the method aspect of the Requirement, the proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this requirement particularly at the Severe VSL category could result in an individual obtaining unauthorized access to BES Cyber Systems. Since the Electronic Security Perimeter is one of the first level of defenses around a network (or dialup modem) containing BES Cyber Systems, any lack of implemented requirements is a binary VSL. The gradation in the VSL is for lacking documentation only. The existence of a particular 'state' regarding documented and implemented processes does not alone constitute the likelihood of exploitation. Several factors centered on intent, motivation, and capabilities and lack of other mitigating controls would necessarily also determine System vulnerability as well as the impact rating of the BES Cyber System in question.
FERC VSL G6 VSLs for cyber security requirements containing	Due to the increased scope of Version 5 and the corresponding increase in the number of declared Electronic Security Perimeters and therefore the order of magnitude more ports and services that will be in scope among other things, the VSL for documentation purposes only has been gradated. Any lapse in the implementation of the actual security controls remains binary.

VRF and VSL Justifications – CIP-005-5, R1	
interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-005-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requirement ensures that interactive remote access to BES Cyber Systems includes documented processes and safeguards to prevent unauthorized access to an entity's networks. Failure to use intermediate devices and establish robust authentication and encryption techniques could result in unauthorized access, which could directly affect the ability to control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for specific intermediate devices to work in conjunction with authentication and encryption procedures for access to BES Cyber Systems. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Use of intermediate devices with proper authentication and encryption procedures for access share a common objective of preventing unauthorized access.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement documented processes and adequate safeguards to prevent unauthorized access to an entity's networks could result in unauthorized access and potential disruption of monitoring and logical control of BES Cyber Assets. Consistent with the definition of a Medium VRF, unauthorized logical access could directly affect the electrical state or the capability of the Bulk Electric System and the ability to monitor and control the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common set of objectives to ensure interactive remote access to BES Cyber Systems is authorized and protected. The obligations to place an inclusive subset of protective measures

VRF and VSL Justifications – CIP-005-5, R2			
	in place to authorize interactive remote access contribute collectively to the objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3.

VRF and VSL Justifications – CIP-005-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This is a new requirement, so this section is not applicable.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-005-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this requirement at the low, moderate, or high VSL category would not necessarily result in an individual obtaining unauthorized interactive remote access to BES Cyber Systems. The existence of a particular 'state' regarding documented and implemented processes does not alone constitute the likelihood of exploitation. Several factors centered on intent, motivation, and capabilities and lack of other mitigating controls would necessarily also determine system vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The action of the requirement is to implement documented cyber security policies. Documentation of the policies is required, but is not the primary objective of the requirement. Documentation is interdependent with the implementation of the policy in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the policy. The drafting team's intent is that this covers both documentation and implementation and,

VRF and VSL Justifications – CIP-005-5, R2	
documentation and implementation should account for their interdependence	therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-006-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this Requirement. The requirement specifies that each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. Failure to restrict physical access to BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets could result in unauthorized access, which could directly affect the ability to monitor or control the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-3, R1, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-5, R1 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-006-5, Requirement R1 requires the implementation of documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control

VRF and VSL Justifications – CIP-006-5, R1			
	Systems and Protected Cyber Assets. A failure to implement these documented plans may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, this requirement, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry and identified deficiencies but did not assess or correct the deficiencies. (1.8) OR	The Responsible Entity has a process to alert for unauthorized physical access to Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process to alert for	The Responsible Entity has a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a	The Responsible Entity did not document or implement operational or procedural controls to restrict physical access. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access and identified deficiencies but did not

VRF and VSL Justifications – CIP-006-5, R1			
The Responsible Entity has a process to log authorized physical entry into any Physical Security Perimeter with sufficient information to identify the individual and date and time of entry but did not identify, assess, or correct the deficiencies. (1.8) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days and identified deficiencies but did not assess or correct the deficiencies. (1.9) OR The Responsible Entity has a process to retain physical access logs for 90 calendar days but did not identify, assess, or correct the deficiencies. (1.9)	unauthorized physical access to Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.7) OR The Responsible Entity has a process communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.7)	process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter but did not identify, assess, or correct deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel and identified deficiencies but did not assess or correct the deficiencies. (1.5) OR The Responsible Entity has a process to communicate alerts within 15 minutes to identified personnel but did not identify, assess, or correct the deficiencies. (1.5) OR The Responsible Entity has a process to monitor for	assess or correct the deficiencies. (1.1) OR The Responsible Entity documented and implemented operational or procedural controls to restrict physical access but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented physical access controls, but at least one control does not exist to restrict access to Applicable Systems. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, and identified deficiencies, but did not assess or

VRF and VSL Justifications – CIP-006-5, R1			
		unauthorized physical access to a Physical Access Control Systems and identified deficiencies but did not assess or correct the deficiencies. (1.6) OR The Responsible Entity has a process to monitor for unauthorized physical access to a Physical Access Control Systems but did not identify, assess, or correct the deficiencies. (1.6)	correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, restricts access to Applicable Systems using at least one control, but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has documented and implemented physical access controls, but at least two different controls do not exist to restrict access to Applicable Systems. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, and identified

VRF and VSL Justifications – CIP-006-5, R1			
			deficiencies, but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity documented and implemented operational or procedural controls, restricts access to Applicable Systems using at least two different controls, but did not identify, assess, or correct the deficiencies. (1.3) OR The Responsible Entity does not have a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter and

VRF and VSL Justifications – CIP-006-5, R1			
			identified deficiencies, but did not assess or correct the deficiencies. (1.4) OR The Responsible Entity has a process to monitor for unauthorized access through a physical access point into a Physical Security Perimeter, but did not identify, assess, or correct the deficiencies. (1.4) OR The Responsible Entity does not have a process to alert for detected unauthorized access through a physical access point into a Physical security Perimeter or to communicate such alerts within 15 minutes to identified personnel. (1.5) OR The Responsible Entity does not have a process to monitor each

VRF and VSL Justifications – CIP-006-5, R1			
			Physical Access Control System for unauthorized physical access to a Physical Access Control Systems. (1.6) OR The Responsible Entity does not have a process to alert for unauthorized physical access to Physical Access Control Systems or to communicate such alerts within 15 minutes to identified personnel(1.7) OR The Responsible Entity does not have a process to log authorized physical entry into each Physical Security Perimeter with sufficient information to identify the individual and date and time of entry. (1.8) OR The Responsible Entity does not have a process to retain physical

VRF and VSL Justifications – CIP-006-5, R1			
			access logs for 90 calendar days. (1.9)

VRF and VSL Justifications – CIP-006-5, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are in line with the currently approved VSLs in previous versions and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-5, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for restricting access have a binary Severe VSL. Other Requirement Parts associated with the physical security plan do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security	Failure to document processes carries a Severe VSL.

VRF and VSL Justifications – CIP-006-5, R1	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-006-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. This Requirement calls for one or more documented visitor control programs. Failure to implement a visitor control program is not expected to directly affect the electrical state or capability of the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented visitor control programs. The VRF is only applied at the requirement level and the requirement parts are treated equally. Each requirement part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-006-3, R1.6, which has an approved VRF of Medium; and, therefore, the proposed VRF for CIP-006-5, R2 is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement a documented visitor control program is an administrative requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The proposed requirement has a single objective of ensuring that Responsible Entities implement one or more documented visitor control programs and, therefore, does not co-mingle more than one obligation.

VRF and VSL Justifications – CIP-006-5, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity included a visitor control program that requires logging of each of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity included a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact and but did not identify, assess, or correct the deficiencies. (2.2) OR	The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter, and identified deficiencies but did not assess or correct deficiencies. (2.1) OR The Responsible Entity included a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter but did not identify, assess, or correct deficiencies. (2.1)	The Responsible Entity has failed to include or implement a visitor control program that requires continuous escorted access of visitors within any Physical Security Perimeter. (2.1) OR The Responsible Entity has failed to include or implement a visitor control program that requires logging of the initial entry and last exit dates and times of the visitor, the visitor's name, and the point of contact. (2.2) OR The Responsible Entity failed to include or implement a visitor control program to retain visitor logs for at least ninety days. (2.3)

VRF and VSL Justifications – CIP-006-5, R2			
	The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days and identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity included a visitor control program to retain visitor logs for at least ninety days but did not identify, assess, or correct the deficiencies. (2.3)		

VRF and VSL Justifications – CIP-006-5, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSL's are in line with the currently approved VSL's in CIP-006-3 and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-5, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the low, moderate, or high VSL category would not necessarily compromise computer network security. The Requirement to further restrict access to only authorized individuals would compensate this control.
FERC VSL G6 VSLs for cyber security	Failure to document processes carries a Severe VSL and therefore recognizes the linkage between documentation and implementation.

VRF and VSL Justifications – CIP-006-5, R2	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-006-5, R3	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. This Requirement calls for one or more documented Physical Access Control System maintenance and testing programs. Failure to implement Physical Access Control System maintenance and testing would not be expected to directly or adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System. A VRF assignment of Lower is, therefore, justified.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for one or more documented Physical Access Control System maintenance and testing programs. The VRF is only applied at the requirement level and the Requirement Parts are treated equally. Each Requirement Part contributes to the reliability objective.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement Physical Access Control System maintenance and testing programs is an administrative Requirement, and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation.

VRF and VSL Justifications – CIP-006-5, R3			
	The proposed Requirement has a single objective of ensuring that Responsible Entities implement one or more Physical Access Control System maintenance and testing programs and, therefore, does not co-mingle more than one obligation.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 24 calendar months but did complete required testing within 25 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 25 calendar months but did complete required testing within 26 calendar months. (3.1)	The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 26 calendar months but did complete required testing within 27 calendar months. (3.1)	The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter. (3.1) OR The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems and locally mounted hardware or devices at the Physical Security Perimeter, but did not complete required testing within 27 calendar months. (3.1)

VRF and VSL Justifications – CIP-006-5, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The VSLs are in line with the currently approved VSLs in CIP-006-3 and therefore do not lower the current compliance level.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-006-5, R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Performing the maintenance activity obligations provides additional assurance in the physical security controls in place, but failure to do so would not necessarily compromise computer network security given other protections. Other Requirement Parts associated with physical security controls do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-006-5, R3	
requirements containing interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R1			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The Requirement is intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and physical I/O ports. Depending on the port and the impact classification of the affected cyber asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the Requirement level, and the Requirement Parts are treated equally. Unprotected logical and physical ports are both access points into a BES Cyber System.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-3, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to disable or prevent access to a single logical or physical port on one BES Cyber System is unlikely to lead to Bulk Electric System instability, separation, or cascading failures. Therefore, this Requirement was assigned a Medium VRF.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. Unprotected logical and physical ports are both access points into a BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has implemented and documented	The Responsible Entity has implemented and documented	The Responsible Entity did not implement or document one or

VRF and VSL Justifications – CIP-007-5, R1			
	processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented and documented processes for Ports and Services but had no methods to protect against unnecessary physical input/output ports used for network connectivity, console commands, or removable media but did not identify, assess, or correct the deficiencies. (1.2)	processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented and documented processes for determining necessary Ports and Services but, where technically feasible, had one or more unneeded logical network accessible ports enabled but did not identify, assess, or correct the deficiencies. (1.1)	more process(es) that included the applicable items in *CIP-007-5 Table R1* and has identified deficiencies but did not assess or correct the deficiencies. (R1) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R1* but did not identify, assess, or correct the deficiencies. (R1)

VRF and VSL Justifications – CIP-007-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-004-3 R2.2, which did not gradate VSLs and treats all violations equally. This version provides more appropriate gradation of the VSLs while still providing a Severe VSL for all types of egregious failures.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement at the moderate or high VSL category would not necessarily compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The Requirement requires entities to manage security patches in a proactive way by monitoring and addressing known security vulnerabilities in software before those vulnerabilities can be exploited in a malicious manner. Depending on the patch and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-007-3, R3, which has an approved VRF of Lower. This version more appropriately assigns a VRF as Medium given other changes in the Requirement. Failure for a given number of individuals to receive training appropriately maps to the severity of the violation.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage a security patch on one BES Cyber System is unlikely to lead to BES instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirement does not co-mingle more than one obligation. It defines required steps in a single process.

VRF and VSL Justifications – CIP-007-5, R2			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking or evaluating cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes, including the identification of sources, for tracking, or evaluating cyber security patches for applicable Cyber	The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* and has identified deficiencies but did not assess or correct the deficiencies. (R2) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R2* but did not identify, assess, or correct the deficiencies. (R2) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber

VRF and VSL Justifications – CIP-007-5, R2			
evaluate the security patches for applicability within 35 calendar days but less than 50 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3)	Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released	documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the source or sources identified and has identified deficiencies but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has documented and implemented one or more process(es) to evaluate uninstalled released security patches for applicability but did not evaluate the security patches for applicability within 65 calendar days of the last evaluation for the days source or sources identified but did not identify, assess, or correct the deficiencies. (2.2)	security patches for applicable Cyber Assets and has identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented or implemented one or more process(es) for patch management but did not include any processes for tracking, evaluating, or installing cyber security patches for applicable Cyber Assets but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate and has identified deficiencies but did not assess or correct the

VRF and VSL Justifications – CIP-007-5, R2			
OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 35 calendar days but less than 50 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	security patches for applicability but did not evaluate the security patches for applicability within 50 calendar days but less than 65 calendar days of the last evaluation for the source or sources identified but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion and has identified deficiencies but did	OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 65 calendar days of the evaluation completion and has identified deficiencies but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or	deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch and documented a revision or extension to the timeframe but did not obtain approval by the CIP Senior Manager or delegate but did not identify, assess, or correct the deficiencies. (2.4) OR The Responsible Entity documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan and has identified deficiencies but did not assess or correct the deficiencies. (2.4) OR The Responsible Entity

VRF and VSL Justifications – CIP-007-5, R2			
	not assess or correct the deficiencies. (2.3) OR The Responsible Entity has one or more documented process(es) for evaluating cyber security patches but, in order to mitigate the vulnerabilities exposed by applicable security patches, did not apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan within 50 calendar days but less than 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	revise an existing mitigation plan within 65 calendar days of the evaluation completion but did not identify, assess, or correct the deficiencies. (2.3)	documented a mitigation plan for an applicable cyber security patch but did not implement the plan as created or revised within the timeframe specified in the plan but did not identify, assess, or correct the deficiencies. (2.4)

VRF and VSL Justifications – CIP-007-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines— There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps to a previously approved VSL for CIP-007-3 R3. The proposed version more appropriately gradates the violation, which is scaled to the risk created by the severity of violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement a security patch can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability. There may be instances where the security vulnerability is so severe that failure to patch alone can comprise computer network security, but these cases are the exception.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R3			
Proposed VRF	**MEDIUM**		
NERC VRF Discussion	The requirement requires entities to have processes to limit and detect the introduction of malicious code onto the components of a BES Cyber System. Depending on the malware and the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the Requirement Parts are treated equally. The parts are required parts of a single process.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-3, R4, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage malicious code on one BES Cyber System is unlikely to lead to BES instability.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
	The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns	The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table*

VRF and VSL Justifications – CIP-007-5, R3			
	are used, the Responsible Entity did not address testing the signatures or patterns and has identified deficiencies but did not assess or correct the deficiencies. (3.3) OR The Responsible Entity has implemented one or more documented process(es), but, where signatures or patterns are used, the Responsible Entity did not address testing the signatures or patterns and did not identify, assess, or correct the deficiencies. (3.3)	not mitigate the threat of detected malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not mitigate the threat of detected malicious code and did not identify, assess, or correct the deficiencies. (3.2) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and has identified deficiencies but did not assess or correct the deficiencies. (3.3)	*R3* and has identified deficiencies but did not assess or correct the deficiencies. (R3) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R3* and did not identify, assess, or correct the deficiencies. (R3) OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and has identified deficiencies but did not assess or correct the deficiencies. (3.1) OR The Responsible Entity has implemented one or more

VRF and VSL Justifications – CIP-007-5, R3			
		OR The Responsible Entity has implemented one or more documented process(es) for malicious code prevention, but where signatures or patterns are used, the Responsible Entity did not update malicious code protections and did not identify, assess, or correct the deficiencies. (3.3)	documented process(es) for malicious code prevention but did not deploy method(s) to deter, detect, or prevent malicious code and did not identify, assess, or correct the deficiencies. (3.1)

VRF and VSL Justifications – CIP-007-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps to a previously approved VSL for CIP-007-3 R4. The proposed version includes a time-based gradation for applying malicious code protection updates which violation intended to match to the degree of severity the violation would pose to the BES.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R3	
Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this Requirement does not necessarily compromise computer network security. Failure to implement malicious code protections can increase the vulnerability of the BES Cyber System, but several other required protections would have to concurrently fail for actuating the vulnerability.
FERC VSL G6 VSLs for cyber security requirements containing	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a process as a Severe violation while also accounting for the failure to implement the process using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R3	
interdependent tasks of documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R4	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	The requirement requires entities to have processes to provide security event monitoring with the purpose of detecting unauthorized access, reconnaissance, and other malicious activity on BES Cyber Systems and comprises of the activities involved with the collection, processing, alerting and retention of security-related computer logs. These logs can provide both (1) the immediate detection of an incident and (2) useful evidence in the investigation of an incident. Depending on the impact classification of the affected Cyber Asset, a violation could lead to affecting the monitoring or control of a BES asset.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The VRF is only applied at the requirement level, and the requirement parts are treated equally. The parts are required parts of a single process.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-007-3, R6, which has an approved VRF of Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to manage security events on one BES Cyber System is unlikely to lead to BES instability.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement does not co-mingle more than one obligation. It defines required steps in a single process.

VRF and VSL Justifications – CIP-007-5, R4			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined	The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined	The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and has identified deficiencies but did not assess or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to generate alerts for necessary security events (as determined by the responsible entity) for the Applicable Systems (per device or	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and has identified deficiencies but did not assess or correct the deficiencies. (R4) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R4* and did not identify, assess, or correct the deficiencies. (R4) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of

VRF and VSL Justifications – CIP-007-5, R4			
summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 22 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	summarization or sampling of logged events at least every 15 calendar days but missed an interval and completed the review within 30 calendar days of the prior review but did not identify, assess, or correct the deficiencies. (4.4)	system capability) but did not generate alerts for all of the required types of events described in 4.2.1 through 4.2.2 and did not identify, assess, or correct the deficiencies. (4.2) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1 (where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and has identified deficiencies but did not assess or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to log applicable events identified in 4.1	the required types of events described in 4.1.1 through 4.1.3 and has identified deficiencies but did not assess or correct the deficiencies. (4.1) OR The Responsible Entity has documented and implemented one or more process(es) to log events for the Applicable Systems (per device or system capability) but did not detect and log all of the required types of events described in 4.1.1 through 4.1.3 and did not identify, assess, or correct the deficiencies. (4.1)

VRF and VSL Justifications – CIP-007-5, R4			
		(where technically feasible and except during CIP Exceptional Circumstances) but did not retain applicable event logs for at least the last 90 consecutive days and did not identify, assess, or correct the deficiencies. (4.3) OR The Responsible Entity has documented and implemented one or more process(es) to identify undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and has identified deficiencies but did not assess or correct the deficiencies. (4.4) OR The Responsible Entity has documented and implemented one or more process(es) to identify	

VRF and VSL Justifications – CIP-007-5, R4			
		undetected Cyber Security Incidents by reviewing an entity-determined summarization or sampling of logged events at least every 15 calendar days but missed two or more intervals and did not identify, assess, or correct the deficiencies. (4.4)	

VRF and VSL Justifications – CIP-007-5, R4	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps to a previously approved VSL for CIP-007-3 R5. The proposed version also includes the new requirement to manually review logs.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R4	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the Requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement Parts for logging required types of events have a binary Severe VSL. Other Requirement Parts associated with security event monitoring do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R4	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-007-5, R5	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities establish, implement, and document controls for electronic access to BES Cyber Systems. This includes enforcement of authentication for all user access and CIP Senior Manager, or delegate authorization for use of administrator, shared, default, and other generic account types. It prescribes procedural controls and conditions for changing default passwords and enforcing specific parameters for password based user authentication. Finally, it helps establish a process to limit (where technically feasible) unsuccessful authentication attempts or generating alerts after a threshold of unsuccessful login attempts.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement calls for specific actions represented by multiple sub-requirements with a common set of objectives – to ensure the appropriate controls are in place for authorizing and establishing secure electronic access to BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007-4 R5, which has an approved VRFs of Lower and Medium; therefore, the proposed VRF is consistent.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement CIP Senior Manager oversight and establish controls to protect BES Cyber Systems from unauthorized electronic access could result in unauthorized access and could directly affect the ability to monitor or control the BES. Although the previous standards versions assigned a VRF of Severe, this is not consistent with the projected risk of BES Cyber System exploitation, which is why the VRF has been modified to Medium.

VRF and VSL Justifications – CIP-007-5, R5			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R5 have a common objective to provide controls to protect against unauthorized electronic access to BES Cyber Systems. The Requirements to authorize and review access, and the provided technical and procedural controls to prevent unauthorized access both specify the obligations to provide strong controls to monitor and control electronic access.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has	The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has	The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and has identified deficiencies but did not assess or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did	The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and has identified deficiencies but did not assess or correct the deficiencies. (R5) OR The Responsible Entity did not implement or document one or more process(es) that included the applicable items in *CIP-007-5 Table R5* and did not identify, assess, or correct the deficiencies. (R5) OR The Responsible Entity has

VRF and VSL Justifications – CIP-007-5, R5			
implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 15 calendar months but less than or equal to 16 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 16 calendar months but less than or equal to 17 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	not include the identification or inventory of all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s) and did not identify, assess, or correct the deficiencies. (5.2) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did not include the identification of the individuals with authorized access to shared accounts and has identified deficiencies but did not assess or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, did	implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and has identified deficiencies but did not assess or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but, where technically feasible, does not have a method(s) to enforce authentication of interactive user access and did not identify, assess, or correct the deficiencies. (5.1) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did

VRF and VSL Justifications – CIP-007-5, R5			
		not include the identification of the individuals with authorized access to shared accounts and did not identify, assess, or correct the deficiencies. (5.3) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce one of the two password parameters as described in 5.5.1 and 5.5.2 and has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access that did not technically or procedurally enforce	not, per device capability, change known default passwords and has identified deficiencies but did not assess or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for System Access Controls but did not, per device capability, change known default passwords but did not identify, assess, or correct the deficiencies. (5.4) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and

VRF and VSL Justifications – CIP-007-5, R5			
		one of the two password parameters as described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for	has identified deficiencies but did not assess or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but the Responsible Entity did not technically or procedurally enforce all of the password parameters described in 5.5.1 and 5.5.2 and did not identify, assess, or correct the deficiencies. (5.5) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last

VRF and VSL Justifications – CIP-007-5, R5			
		password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 17 calendar months but less than or equal to 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6)	password change and has identified deficiencies but did not assess or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for password-only authentication for interactive user access but did not technically or procedurally enforce password changes or an obligation to change the password within 18 calendar months of the last password change and did not identify, assess, or correct the deficiencies. (5.6) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or

VRF and VSL Justifications – CIP-007-5, R5			
			generate alerts after a threshold of unsuccessful authentication attempts and has identified deficiencies but did not assess or correct the deficiencies. (5.7) OR The Responsible Entity has implemented one or more documented process(es) for System Access Control but, where technically feasible, did not either limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts and did not identify, assess, or correct the deficiencies. (5.7)

VRF and VSL Justifications – CIP-007-5, R5	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The previous binary VSL for this Requirement has not proven accurate after several iterations of its application. Account access management and procedures for monitoring and controlling access are complex with an often intensive scope. Errors resulting in potential or single instances of unauthorized access do not have the same criticality as multiple instances and blatant lack of controls.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-007-5, R5	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations. Gradations are based on the number of unidentified account types, or number of missed controls for authentication and access represent components of the overall requirement that are necessary to fully achieve the reliability of the main requirement.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The Requirement parts that can compromise computer network security have a Severe VSL. Other Requirement Parts associated with system access control do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-007-5, R5	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R1	
Proposed VRF	**LOWER**
NERC VRF Discussion	This requires each Responsible Entity to have a plan to respond to Cyber Security Incidents. Failure to have an incident response plan could delay recovery actions and hinder entities in understanding and reporting the incident. The planning component of the Requirement is administrative in nature and, if violated, would not be expected to affect the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to respond to Cyber Security Incidents. The VRF is only applied at the requirement level and the Requirement Parts are treated equally. Each requirement part is a necessary component of an incident response plan.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1, which has an approved VRF of Lower.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have an incident response plan could delay recovery actions and hinder entities in understanding and reporting the incident. The planning component of the Requirement is administrative in nature and, if violated, would not be expected to affect the BES.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common objective of having a plan for responding to, handling, and reporting Cyber Security Incidents. These contribute to the overall objective to minimize the loss and destruction of Cyber Security Incidents and providing timely information about the incident.

VRF and VSL Justifications – CIP-008-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include the roles and responsibilities of Cyber Security Incident response groups or individuals. (1.3) OR The Responsible Entity has developed the Cyber Security Incident response plan(s), but the plan does not include incident handling procedures for Cyber Security Incidents. (1.4)	The Responsible Entity has not developed a Cyber Security Incident response plan with one or more processes to identify, classify, and respond to Cyber Security Incidents. (1.1) OR The Responsible Entity has developed a Cyber Security Incident response plan, but the plan does not include one or more processes to identify Reportable Cyber Security Incidents. (1.2) OR The Responsible Entity has developed a Cyber Security Incident response plan, but did not provide at least preliminary notification to ES-ISAC within one hour from identification of a Reportable Cyber Security

VRF and VSL Justifications – CIP-008-5, R1			
			Incident. (1.2)

VRF and VSL Justifications – CIP-008-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this Requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps from CIP-008-3 R1 and has similar VSL assignments. The previously approved VSL differentiated between High and Severe on the basis of whether the entity had maintained the plan. The change made to this version differentiates based on specific components of the plan, which provides more objectivity.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-008-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement indicates an entity does not have a documented and consistent response to a Cyber Security Incident, but a single lapse in protection would not be expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-008-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures entities implement their incident response plan(s). Failure to implement the incident response plan is an administrative requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of implementing the incident response plan. The Requirement to retain incident documentation ensures the entity can review actual incidents at a later date.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1.6 and R2, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement the incident response plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R2 have a common objective of implementing incident response plans. Requirement Row 2.1 specifies the obligation to implement the plan during an incident, and Requirement Row 2.2 specifies the obligation to periodically exercise the plan. Requirement Row 2.3 specifies the obligation to retain incident documentation to ensure the entity can review actual incidents at a later date.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not	The Responsible Entity has not	The Responsible Entity has not	The Responsible Entity has not

VRF and VSL Justifications – CIP-008-5, R2			
tested the Cyber Security Incident response plan(s) within 15 calendar months, not exceeding 16 calendar months between tests of the plan. (2.1)	tested the Cyber Security Incident response plan(s) within 16 calendar months, not exceeding 17 calendar months between tests of the plan. (2.1)	tested the Cyber Security Incident response plan(s) within 17 calendar months, not exceeding 18 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)	tested the Cyber Security Incident response plan(s) within 19 calendar months between tests of the plan. (2.1) OR The Responsible Entity did not retain relevant records related to Reportable Cyber Security Incidents. (2.3)

VRF and VSL Justifications – CIP-008-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed version more appropriately gradates the violation, which is scaled to the risk created by the severity of violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-008-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	This requirement maps from CIP-008-3 R1 and has similar VSL assignments. The previously approved VSL was binary. The change made to this version differentiates based on the number of days late in a time-based performance. This reflects the lesser degree of risk posed to BES reliability for exceeding timed requirements. New requirements have also been incorporated into the VSL.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection of this Requirement does not compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-008-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-008-5, R3			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures incident response plans remain up-to-date and that individuals with responsibilities in the plans have the most current version.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of keeping response plans up-to-date and communicating changes to individuals with responsibilities in the plans. The obligations to keep the response plans up-to-date include changes in response to lessons learned in an incident or organizational and technology changes.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-008-3 R1.4 and R1.5, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to update and communicate changes to the incident response plan(s) are administrative requirements and are not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common objective of keeping response plans up-to-date and communicating changes to individuals with responsibilities in the plans.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not notified each person or group with a defined role in the Cyber	The Responsible Entity has not updated the Cyber Security	The Responsible Entity has neither documented lessons learned nor	The Responsible Entity has neither documented lessons learned nor

VRF and VSL Justifications – CIP-008-5, R3			
Security Incident response plan of updates to the Cyber Security Incident response plan within greater than 90 but less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3)	Incident response plan based on any documented lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the Cyber Security Incident response plan of updates to the Cyber Security Incident response plan within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.3) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 60	documented the absence of any lessons learned within 90 and less than 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1) OR The Responsible Entity has not updated the Cyber Security Incident response plan based on any documented lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.2) OR The Responsible Entity has not updated the Cyber Security Incident response plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the	documented the absence of any lessons learned within 120 calendar days of a test or actual incident response to a Reportable Cyber Security Incident. (3.1.1)

VRF and VSL Justifications – CIP-008-5, R3			
	and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	ability to execute the plan: (3.2) • Roles or responsibilities, or • Cyber Security Incident response groups or individuals, or • Technology changes.	

VRF and VSL Justifications – CIP-008-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this Requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement has more specificity about reviewing and updating the plan than prior versions of the standard, and the failure to update the plan in a timely manner has less of an impact than not performing the review at all.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-008-5, R3	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement should not compromise the security of the BES Cyber System because this is in response to an incident which has already occurred,
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-008-5, R3	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This requires each Responsible Entity have a plan to recover to BES Cyber Systems. Failure to have a recovery plan could increase the downtime and destruction in a hazardous situation, which could affect the ability to effectively monitor, control, or restore the Bulk Electric System in an Emergency situation.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for procedures to recover BES Cyber Systems. The VRF is only applied at the requirement level, and the requirement parts are treated equally. Each Requirement Part is a necessary component of a recovery plan.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps from CIP-009-3 R1, which has an approved VRF of Medium.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to have a recovery plan could increase the downtime and destruction in a hazardous situation, which could affect the ability to effectively monitor, control, or restore the Bulk Electric System in an Emergency situation.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R1 have a common objective of having a plan for recovering BES Cyber Systems. These contribute to the overall objective to minimize downtime and destruction in a hazardous situation. T he requirement to preserve data during recovery provides information for post-event analysis, but this requirement best fits here because it involves the actions taken during recovery.

VRF and VSL Justifications – CIP-009-5, R1			
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address one of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has developed recovery plan(s), but the plan(s) do not address two of the requirements included in Parts 1.2 through 1.5.	The Responsible Entity has not created recovery plan(s) for BES Cyber Systems. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address the conditions for activation in Part 1.1. OR The Responsible Entity has created recovery plan(s) for BES Cyber Systems, but the plan(s) does not address three or more of the requirements in Parts 1.2 through 1.5.

VRF and VSL Justifications – CIP-009-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this Requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This Requirement maps from CIP-009-3 R1, and has similar VSL assignments. The previously approved VSL did not have a differentiation between having a plan and missing some elements of the plan, but the severity of not having a plan is higher than missing a single element in a plan.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-009-5, R1	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement indicates an entity has not created recovery plan(s) for BES Cyber Systems, but a single lapse in protection would not be expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This requirement only specifies documentation, and not implementation.

VRF and VSL Justifications – CIP-009-5, R1	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R2			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement's VRF is consistent with similar administrative Requirements with similar risks in other NERC Reliability Standards.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of implementing and maintaining the recovery plan.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This requirement maps from CIP-009-3 R2, R4, and R5, which has an approved VRF of Lower.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to implement and maintain the recovery plan is an administrative Requirement and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirements in R2 have a common objective of implementing and maintaining recovery plans. Requirement Rows 2.1 and 2.3 specify the obligation to implement and test the plan. Requirement Row 2.2 specifies the obligation to maintain backup information used to recover the BES Cyber System.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within	The Responsible Entity has not tested the recovery plan(s) within 16 calendar months, not	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 17	The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.1 within 18

VRF and VSL Justifications – CIP-009-5, R2			
15 calendar months, not exceeding 16 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 15 calendar months, not exceeding 16 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 36 calendar months, not exceeding 37 calendar months	exceeding 17 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 16 calendar months, not exceeding 17 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 37 calendar months, not exceeding 38 calendar months between tests, and when	calendar months, not exceeding 18 calendar months between tests of the plan, and when tested, any deficiencies were identified, assessed, and corrected. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 17 calendar months, not exceeding 18 calendar months between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.2) OR The Responsible Entity has not tested the recovery plan according to R2 Part 2.3 within 38 calendar months, not exceeding 39 calendar months between tests, and when tested, any deficiencies were identified, assessed, and	calendar months between tests of the plan. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 and identified deficiencies, but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.1 but did not identify, assess, or correct the deficiencies. (2.1) OR The Responsible Entity has not tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 within 18 calendar months between tests. (2.2) OR

VRF and VSL Justifications – CIP-009-5, R2			
between tests, and when tested, any deficiencies were identified, assessed, and corrected. (2.3)	tested, any deficiencies were identified, assessed, and corrected. (2.3)	corrected. (2.3)	The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 and identified deficiencies, but did not assess or correct the deficiencies. (2.2) OR The Responsible Entity has tested a representative sample of the information used in the recovery of BES Cyber System functionality according to R2 Part 2.2 but did not identify, assess, or correct the deficiencies. (2.2) OR The Responsible Entity has not tested the recovery plan(s) according to R2 Part 2.3 within 39 calendar months between tests of the plan. (2.3) OR

VRF and VSL Justifications – CIP-009-5, R2			
			The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 and identified deficiencies, but did not assess or correct the deficiencies. (2.3) OR The Responsible Entity has tested the recovery plan(s) according to R2 Part 2.3 but did not identify, assess, or correct the deficiencies. (2.3)

VRF and VSL Justifications – CIP-009-5, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The Requirement maps to CIP-009-3 R2 and R3 and adds the obligation to perform a full operational exercise. The portions of the Requirement from CIP-009-3 carry forward similar VSLs, and the failure to perform a full operational exercise is proposed as a High VSL because it does not carry the same potential consequence of not having exercised the recovery plan. In addition, the proposed VSLs gradate failure to perform a test of the recovery plan based on the amount of time lapse between tests. This more appropriately reflects the severity of the corresponding type of violation.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF and VSL Justifications – CIP-009-5, R2	
Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A violation of this requirement indicates the recovery plan was not properly tested and may have deficiencies, but a violation cannot immediately compromise computer security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of	This Requirement does not specify a lower VSL for lack of documentation.

VRF and VSL Justifications – CIP-009-5, R2	
documentation and implementation should account for their interdependence	

VRF and VSL Justifications – CIP-009-5, R3			
Proposed VRF	**LOWER**		
NERC VRF Discussion	This Requirement ensures BES Cyber System plans remain up-to-date and effective and that individuals with responsibilities in the plans have the most current version.		
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A		
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. Each Requirement row contributes to the common objective of keeping recovery plans up-to-date and effective.		
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. The assignment of a Lower VRF is consistent of the impact of a violation of this Requirement and is therefore consistent among Reliability Standards.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to review, update or communicate changes to the recovery plan is administrative in nature and is not expected to adversely affect the electrical state or capability of the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The Requirements in R2 have a common objective of keeping response plans up-to-date and effective.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 90 and less than 210 calendar days of the	The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 90 and less than 210 calendar days of	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 90 and less than 210 calendar days of each	The Responsible Entity has neither documented lessons learned nor documented the absence of any lessons learned within 210 calendar days of

VRF and VSL Justifications – CIP-009-5, R3			
update being completed. (3.1.3)	each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not notified each person or group with a defined role in the recovery plan(s) of updates within 120 calendar days of the update being completed. (3.1.3) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 60 and less than 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or • Technology changes.	recovery plan test or actual recovery. (3.1.1) OR The Responsible Entity has not updated the recovery plan(s) based on any documented lessons learned within 120 calendar days of each recovery plan test or actual recovery. (3.1.2) OR The Responsible Entity has not updated the recovery plan(s) or notified each person or group with a defined role within 90 calendar days of any of the following changes that the responsible entity determines would impact the ability to execute the plan: (3.2) • Roles or responsibilities, or • Responders, or Technology changes.	each recovery plan test or actual recovery. (3.1.1)

VRF and VSL Justifications – CIP-009-5, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement has more specificity about reviewing and updating the plan than prior versions of the standard, and the failure to update the plan in a timely manner has less of an impact than not performing the review at all.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are,

VRF and VSL Justifications – CIP-009-5, R3	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	therefore, consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and are not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single violation of this Requirement should not compromise the security of the BES Cyber System because this is in response to an incident which has already occurred.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	The VSLs account for the interdependence of documentation and implementation and treats the failure to document a program as a Severe violation while also accounting for the failure to implement the program using a gradation VSL methodology.

VRF and VSL Justifications – CIP-010-1, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration change management processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration change management processes can have a medium impact on the reliability and operability of the BES. Although the requirement is administrative in nature and is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration change management. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-1, R1 specifies the implementation of documented configuration change management processes in conjunction with CIP-010-1, R2, which specifies the implementation of documented configuration monitoring processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-1, Requirement R1 requires the implementation of documented configuration change

VRF and VSL Justifications – CIP-010-1, R1			
	management processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, poses the potential to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-1, Requirement R1 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies.	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)

VRF and VSL Justifications – CIP-010-1, R1			
OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes all of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration and identified deficiencies in the verification documentation but did not assess or correct the deficiencies. (1.4.3) OR The Responsible Entity has a process(es) to perform steps in 1.4.1 and 1.4.2 for a change(s) that deviates from the existing baseline configuration but did not	did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes four of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration and identified deficiencies in the determination of affected security controls, but did not assess, or correct the	(1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes three of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify, assess, and correct the deficiencies. (1.1) OR The Responsible Entity has a process(es) that requires authorization and documentation for changes that deviate from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) that requires authorization and	OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 and identified deficiencies but did not assess and correct the deficiencies. (1.1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes two or fewer of the required baseline items listed in 1.1.1 through 1.1.5 but did not identify,

VRF and VSL Justifications – CIP-010-1, R1			
identify, assess, or correct the deficiencies in the verification documentation. (1.4.3)	deficiencies. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the determination of affected security controls. (1.4.1)	documentation for changes that deviate from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.2) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration and identified deficiencies but did not assess or correct the deficiencies. (1.3) OR The Responsible Entity has a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies. (1.3)	assess, and correct the deficiencies. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity

VRF and VSL Justifications – CIP-010-1, R1			
		OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration and identified deficiencies in required controls, but did not assess, or correct the deficiencies. (1.4.2) OR The Responsible Entity has a process(es) to verify that required security controls in CIP-005 and CIP-007 are not adversely affected by a change(s) that deviates from the existing baseline configuration but did not identify, assess, or correct the deficiencies in the required controls. (1.4.2) OR The Responsible Entity has a	does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected

VRF and VSL Justifications – CIP-010-1, R1			
		process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration, and identified deficiencies but did not assess or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration but did not identify, assess, or correct the deficiencies. (1.5.1) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments	following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

VRF and VSL Justifications – CIP-010-1, R1			
		and identified deficiencies but did not assess or correct the deficiencies. (1.5.2) OR The Responsible Entity has a process to document the test results and, if using a test environment, document the differences between the test and production environments, but did not identify, assess, or correct the deficiencies. (1.5.2)	

VRF and VSL Justifications – CIP-010-1, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement is new and has no mapping to a Requirement in a previous NERC CIP Standards Version. It does not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore,

VRF and VSL Justifications – CIP-010-1, R1	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-1, Requirement R1 specifies that a Responsible Entity must implement and document the processes for configuration change management of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration change management process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-1, R2	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The requirement calls for the implementation of one of more documented configuration monitoring processes. A VRF assignment of Medium is consistent with the lower risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration. The impact of a failure to implement documented configuration monitoring processes has medium impact on the reliability and operability of the BES.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented processes in relation to configuration monitoring. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to prevent unauthorized modifications to BES Cyber Assets and BES Cyber Systems based on their baseline configuration.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. CIP-010-1, R2 specifies the implementation of documented configuration monitoring processes in conjunction with CIP-010-1, R1, which specifies the implementation of documented configuration change management processes. Both requirements have a medium risk impact of a violation to implement their documented processes and, therefore, have a Medium VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-1, Requirement R2 requires the implementation of documented configuration monitoring processes. A failure to implement these documented processes has medium impact on the reliability and operability of the BES.

VRF and VSL Justifications – CIP-010-1, R2			
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-1, Requirement R2 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1) OR The Responsible Entity has documented and implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days and identified deficiencies but did not assess or correct the deficiencies. (2.1) OR The Responsible Entity has documented and implemented a

VRF and VSL Justifications – CIP-010-1, R2			
			process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days but did not identify, assess, or correct the deficiencies. (2.1)

VRF and VSL Justifications – CIP-010-1, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines — Severe: the performance measured does not substantively meet the intent of the Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed Requirement is new and has no mapping to a Requirement in a previous NERC CIP Standards Version. It does not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSL is binary and assigns a "Severe" category for the violation of the Requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated Requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-010-1, R2	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	The VSL is binary.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-1, Requirement R2 specifies that a Responsible Entity must implement and document the processes for configuration monitoring of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the configuration monitoring process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-010-1, R3	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	A VRF of Medium is assigned to this requirement. The Requirement calls for the implementation of one of more documented vulnerability assessment processes. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls of BES Cyber Assets and BES Cyber Systems. Failure to implement vulnerability assessment processes may impact the reliability and operability of the BES. The requirement is a requirement that, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. The requirement calls for the implementation of one of more documented vulnerability assessment processes. The VRF is only applied at the requirement level and the requirement parts are treated equally. A VRF assignment of Medium is consistent with the medium risk impact of a violation to implement documented processes that are intended to act as a component in an overall program to periodically ensure the proper implementation of security controls of BES Cyber Assets and BES Cyber Systems.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. Requirement Part 3.1 maps from CIP-005-4, R4 (which has an assigned VRF of Medium) and CIP-007-4, R8 (which has an assigned VRF of Lower), Requirement Part 3.2 is a new requirement, while Requirement Part 3.3 maps from CIP-005-4, R4.5 (which has an assigned VRF of Medium) and CIP-007-4, R8.4 (which has an assigned VRF of Medium). Most of the aforementioned requirements had an approved VRF of Medium and, therefore, the proposed VRF for CIP-010-1, R3 is consistent. While the drafting team

VRF and VSL Justifications – CIP-010-1, R3			
	recognizes that CIP-007-4, R8 was assigned a VRF of Lower, to maintain consistency among reliability standards, an assigned VRF of Medium is appropriate.		
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. CIP-010-1, Requirement R3 requires the implementation of documented vulnerability assessment processes. A failure to implement these documented processes may impact the reliability and operability of the BES. Therefore, and according to NERC VRF definitions, the requirement is a requirement that, if violated, could directly affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. CIP-010-1, Requirement R3 addresses a single objective and has a single VRF.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months

VRF and VSL Justifications – CIP-010-1, R3			
documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3)

VRF and VSL Justifications – CIP-010-1, R3			
			OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)

VRF and VSL Justifications – CIP-010-1, R3	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The proposed requirement is mapped to Requirement R4 and R4.5 of CIP-005-4 and Requirement R8 and R8.4 of CIP-007-4. Additionally, Requirement Part 3.2 is a new requirement and has no mapping to a Requirement in a previous NERC CIP Standards Version. The binary VSL for the previous releases were based on performing vulnerability assessments annually, or not including one or more of the various elements identified in the related sub-requirements in a vulnerability assessment. This version's VSLs have evolved from this binary component model to a multidimensional component model. The proposed requirement does not have the unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the Requirement.

VRF and VSL Justifications – CIP-010-1, R3	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	This Requirement seeks to implement vulnerability assessment processes that if not done may impact the reliability and operability of the BES, but a single lapse in protection is not expected to compromise computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	CIP-010-1, Requirement R3 specifies that a Responsible Entity must implement and document the processes for vulnerability assessments of BES Cyber Assets and BES Cyber Systems. Documentation of these processes is required, but this documentation is not the primary objective of the requirement. Documentation is interdependent with the implementation of the processes in this case. As such, the VSL measures distance from compliance in terms of whether or not the Responsible Entity "addressed" all the required elements of the vulnerability assessment process. The drafting team's intent is that this covers both documentation and implementation and, therefore, accounts for the interdependence of these tasks.

VRF and VSL Justifications – CIP-011-5, R1	
Proposed VRF	**MEDIUM**
NERC VRF Discussion	This Requirement ensures that Responsible Entities prevent unauthorized access to BES Cyber System Information. Failure to adequately identify, protect, and control access to such information could result in unauthorized access and lost, stolen, or misused Cyber System Information. Such failure represents a risk to the Bulk Electric System.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This requirement calls for methods to identify, provide secure handling, and control access to Cyber System Information. The VRF is only applied at the requirement level and the requirement parts are treated equally. The identification, secure handling and control of access have the common objective to protect BES Cyber System Information.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-003, R4 and CIP-003-3, R4.1, which have an approved VRF of Medium. The Requirement also maps to CIP-003-3, R4.2 and CIP-003-3, R4.3 and to CIP-003-3, R5, CIP-003-3, R5.1, CIP-003-3, R5.2, and CIP-003-3, R5.3, which have an approved VRF of Lower. The requirement has the object of securing Cyber System Information. Version 5 combines requirements to ensure consistency. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately identify and protect BES Cyber System Information could result in disclosure of information to unauthorized persons, lost, stolen, or misused Cyber System Information. Such breaches of confidentiality represent a risk to the reliability of Bulk Electric System from misuse by unauthorized persons.
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The sub requirements in R1 have a common objective to assure confidentiality of BES Cyber System

VRF and VSL Justifications – CIP-011-5, R1			
	Information. The obligations to identify, control access, and assure proper handling of BES Cyber System Information contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more methods to identify BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.1) OR The Responsible Entity has implemented a BES Cyber System	The Responsible Entity has not documented or implemented a BES Cyber System Information protection program (R1).

VRF and VSL Justifications – CIP-011-5, R1			
		Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information and has identified deficiencies but did not assess or correct the deficiencies. (1.2) OR The Responsible Entity has implemented a BES Cyber System Information protection program which includes one or more procedures for protection and secure handling BES Cyber System Information but did not identify, assess, or correct the deficiencies. (1.2)	

VRF and VSL Justifications – CIP-011-5, R1	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this Requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The previously approved VSLs included a combination of binary and gradated VSLs. The Proposed VSLs are consistent with the approved VSLs for the CIP 011-5 R1 requirement, which maps to CIP 004-3, R4 and CIP 004-3, R5.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement.

VRF and VSL Justifications – CIP-011-5, R1	
Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document and implement a BES Cyber System information protection program has a binary Severe VSL. Other Requirement Parts associated with the information protection program do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Interdependent tasks of documentation, identification, and implementation are treated in a uniform manner and have not been separated for each topical area addressed in the requirement.

VRF and VSL Justifications – CIP-011-1, R2	
Proposed VRF	**LOWER**
NERC VRF Discussion	A VRF of Lower is assigned to this requirement. This requirement ensures that Responsible Entities take action to prevent unauthorized retrieval of BES Cyber System information prior to disposal or reuse of asset storage media. A violation would not be expected to affect the electrical state or capability of the Bulk-Power System or the ability to effectively monitor and control the Bulk-Power System. Several other factors, including capabilities and intention of the individual and lack of other mitigating controls, would be required to make the BES Cyber System vulnerable. Therefore, the VRF of lower is consistent with the NERC definition of VRFs.
FERC VRF G1 Discussion	Guideline 1- Consistency with Blackout Report. N/A
FERC VRF G2 Discussion	Guideline 2- Consistency within a Reliability Standard. This Requirement ensures that Responsible Entities take action to prevent unauthorized retrieval of BES Cyber System Information prior to disposal or reuse of asset storage media. The VRF is only applied at the requirement level and the requirement parts are treated equally. R2.1. calls for the Responsible Entity to take action to prevent unauthorized retrieval of BES Cyber System Information at the time of reuse. R2.2. mandates that Responsible Entities take action to prevent unauthorized retrieval of such information at the time of disposal. The VRF of lower is consistent with the risk of a violation across the requirement parts.
FERC VRF G3 Discussion	Guideline 3- Consistency among Reliability Standards. This Requirement maps to CIP-007 R7, which has a VRF of Lower. The Requirement has the object of preventing unauthorized retrieval of BES Cyber System Information from asset media prior to reuse or disposal. The proposed VRF is consistent with the approved VRF.
FERC VRF G4 Discussion	Guideline 4- Consistency with NERC Definitions of VRFs. Failure to adequately protect information contained in asset storage media during reuse or disposal would not be expected to affect the electrical state or capability of the Bulk Power System or the ability to

VRF and VSL Justifications – CIP-011-1, R2			
	effectively monitor or control the Bulk-Power System. Several other factors, including capabilities and intention of the individual and lack of other mitigating controls, would be required to make the BES Cyber System vulnerable. Therefore, the VRF of lower is consistent with the NERC definition of VRFs.		
FERC VRF G5 Discussion	Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation. The requirement/sub-requirements in R2 have a common objective to assure confidentiality of BES Cyber System Information. The obligations to protect such information, which may be contained on asset media, during both reuse and destruction, contribute to this objective and only one VRF is assigned.		
Proposed VSLs			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity implemented one or more documented processes but did not include processes for reuse as to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.1)	The Responsible Entity implemented one or more documented processes but did not include disposal or media destruction processes to prevent the unauthorized retrieval of BES Cyber System Information from the BES Cyber Asset. (2.2)	The Responsible Entity has not documented or implemented any processes for applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. (R2)

VRF and VSL Justifications – CIP-011-1, R2	
NERC VSL Guidelines	Meets NERC's VSL Guidelines—There is an incremental aspect to a violation of this requirement and the VSLs follow the guidelines for incremental violations. Some measurable reliability benefit can be achieved if the Responsible Entity documented cyber security policies but fails to address one or more of the required elements of the cyber security policy. The drafting team has, therefore, decided that gradated performance VSLs are appropriate for this requirement.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The previously approved VSLs included a combination of binary and gradated VSLs. The proposed VSLs are consistent with the approved VSLs for the CIP-007 R7 requirement, which maps to this requirement. There is no unintended consequence of lowering the current level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	The proposed VSLs are not binary and do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3	The proposed VSLs use the same terminology as used in the associated requirement and are, therefore, consistent with the requirement. The VSL does not expand the requirement.

VRF and VSL Justifications – CIP-011-1, R2	
Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSLs are based on a single violation, and not cumulative violations.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Failure to document or implement all required processes has a binary Severe VSL. Other Requirement Parts associated with the required processes do not indicate a single lapse compromising computer network security.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	Interdependent tasks of documentation, identification, and implementation are treated in a uniform manner and have not been separated for each topical area addressed in the requirement.