UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, AND CIP-011-2

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

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charles.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

February 13, 2015

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation	**)** **)**	**Docket No. _____**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, AND CIP-011-2

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA"),[1] Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] and Order No. 791,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval the following proposed Critical Infrastructure Protection ("CIP") Reliability Standards:

- CIP-003-6 – Cyber Security – Security Management Controls
- CIP-004-6 – Cyber Security – Personnel and Training
- CIP-006-6 – Cyber Security – Physical Security of BES Cyber Systems
- CIP-007-6 – Cyber Security – Systems Security Management
- CIP-009-6 – Cyber Security – Recovery Plans for BES Cyber Systems
- CIP-010-2 – Cyber Security – Configuration Change Management and Vulnerability Assessments
- CIP-011-2 – Cyber Security – Information Protection

---

1 16 U.S.C. § 824o (2006).

2 18 C.F.R. § 39.5 (2014).

3 *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and rehearing*, Order No. 791-A, 146 FERC ¶ 61, 188 (2014).

4 The Commission certified NERC as the electric reliability organization ("ERO") in accordance with Section 215 of the FPA on July 20, 2006. *N. Am. Elec. Reliability Corp.*, 116 FERC ¶ 61,062 (2006).

NERC requests that the Commission approve the proposed Reliability Standards, provided in Exhibit A hereto, as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

NERC also requests approval of:

- the associated Implementation Plan (Exhibit B);
- the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and E);
- the proposed new or revised definitions to be incorporated into the NERC Glossary of Terms Used in Reliability Standards ("NERC Glossary") for the following terms: (1) BES Cyber Asset, (2) Protected Cyber Asset ("PCA"), (3) Low Impact BES Cyber System Electronic Access Point ("LEAP"), (4) Low Impact External Routable Connectivity ("LERC"); (5) Removable Media, and (6) Transient Cyber Asset (Exhibit A); and
- the retirement of Commission-approved Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1.

As required by Section 39.5(a) of the Commission's regulations,[5] this Petition presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (Exhibit F), and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672[6] (Exhibit C). The NERC Board of Trustees ("Board") adopted proposed Reliability Standards CIP-006-6 and CIP-009-6 on November 13, 2014 and proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 on February 12, 2015.[7]

---

[5] 18 C.F.R. § 39.5(a) (2013).

[6] *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 262, 321-37, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[7] Unless otherwise designated, all capitalized terms used herein shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

I. EXECUTIVE SUMMARY

The purpose of NERC's CIP cybersecurity Reliability Standards is to mitigate the cybersecurity risks to Bulk Electric System Facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cyber-attack, would affect the reliable operation of the Bulk Electric System. On November 22, 2013, the Commission issued Order No. 791, approving new and modified CIP cybersecurity Reliability Standards, collectively referred to as the CIP Version 5 Standards, to become effective on April 1, 2016.[8] As the Commission stated, the CIP Version 5 Standards represent an improvement over the currently-effective CIP Reliability Standards as they adopt new cybersecurity controls and extend the scope of the systems protected by the CIP Reliability Standards.[9] While the Commission approved the CIP Version 5 Standards, it also directed NERC to develop the following modifications to improve those standards:

1. Modify or remove the language in 17 requirements in the CIP Version 5 Standards that requires responsible entities to implement cyber security policies in a manner that "identifies, assesses, and corrects deficiencies."[10]

2. Develop modifications to the CIP Version 5 Standards to address security controls for low impact BES Cyber Systems.[11]

3. Develop requirements that protect transient devices (e.g., thumb drives, laptop computers, and other devices that are portable and frequently connected and disconnected from systems on a temporary basis) that fall outside the definitions for BES Cyber Asset and PCA.[12]

4. Create a definition of "communication networks" and develop new or modified standards that address the protection of the nonprogrammable components of communication networks.[13]

---

[8] The Commission also approved 19 new or revised defined terms used in the CIP Version 5 Standards for incorporation into the NERC Glossary.

[9] Order No. 791 at PP 1-2; 41.

[10] *Id*. at PP 4, 67-76.

[11] *Id*. at PP 5, 106-110.

[12] *Id*. at PP 6, 132-136.

[13] *Id*. at PP 7, 148-150.

The Commission directed NERC to submit for Commission approval revised standards addressing the "identify, assess, and correct" and communication networks directives within one year from the effective date of Order No. 791, which is February 3, 2015.[14] On January 13, 2015, the Commission granted NERC a 10-day extension of the February 3, 2015 deadline.[15] The Commission did not provide a deadline for the directives related to low impact BES Cyber Systems and transient devices.

As discussed further below, the proposed Reliability Standards improve the cybersecurity protections required by the CIP Reliability Standards and collectively address the Commission's four directives from Order No. 791 as follows:

"Identify, Assess, and Correct" Language – Consistent with the Commission's directive, NERC has removed the "identify, assess, and correct" language from the 17 requirements in the CIP Version 5 Standards that included such language.[16] NERC is addressing the concerns underlying the "identify, assess, and correct" language outside the text of a Reliability Standard as part of its risk-based Compliance Monitoring and Enforcement Program ("CMEP"). Specifically, in 2012, NERC launched the Reliability Assurance Initiative ("RAI"), a multi-year effort to identify and implement changes to enhance the effectiveness of the ERO's CMEP by establishing a robust, risk-based approach to compliance monitoring and enforcement. Consistent with the fundamental rationale and principles of the "identify, assess, and correct" language, the purpose of RAI was to design and implement a risk-based CMEP that, among other things: (1) focuses on

[14] Order No. 791 was published in the Federal Register on December 3, 2013 and became effective on February 3, 2014.

[15] *Notice Granting Extension of Time*, Docket No. RM13-5-000 (Jan. 13, 2015).

[16] Those 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5.1, Requirements R2, R3, R4, and R5; CIP-006-5, Requirements R1 and R2; CIP-007-5, Requirements R1, R2, R3, R4, and R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

improving entities' internal controls; (2) scopes compliance monitoring activities based on risk assessments; (3) provides appropriate deterrence through enforcement; and (4) establishes a feedback loop to improve the content of the Reliability Standards. As discussed in NERC's informational filing in Docket No. RR15-2-000, through RAI, NERC developed a risk-based CMEP that includes processes and programs, such as risk assessments, compliance exceptions, and self-logging of minimal risk issues, that directly accomplish the goals of the "identify, assess, and correct" language.[17] In 2015, NERC began to implement these new risk-based processes and programs for all registered entities.

Security Controls for Assets Containing Low Impact BES Cyber Systems – In response to the Commission's concern that the CIP Version 5 Standards do not contain specific controls for low impact BES Cyber Systems or objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities for their low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6, Requirement R2 requires responsible entities to implement cybersecurity plans for assets containing low impact BES Cyber Systems to meet specific security objectives related to: (i) cybersecurity awareness; (ii) physical security controls; (iii) electronic access controls; and (iv) Cyber Security Incident response. Considering the large number and wide variety of types of low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6 provides responsible entities the flexibility to implement security controls in the manner that best suits the needs and characteristics of their organization. By articulating clear security objectives for each of the four subject matter areas listed above, however, the ERO and

[17] *See* Informational Filing of the North American Electric Reliability Corporation, Docket No. RR15-2-000 (November 3, 2014) (the "RAI Informational Filing).

the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity.

Additionally, proposed Reliability Standard CIP-003-6, Requirement R1 requires responsible entities to document cybersecurity policies for their assets containing low impact BES Cyber Systems and for the policies to be reviewed and approved by the CIP Senior Manager. The policies must cover the same four areas as the Requirement R2 plans: cybersecurity awareness; physical security controls; electronic access controls; and Cyber Security Incident response. These policies, like the policies already required for high and medium impact BES Cyber Systems, will communicate the responsible entity's management goals, objectives, and expectations for the protection of low impact BES Cyber Systems. These policies will help establish an overall governance foundation for creating a culture of security and compliance.

Protection of Transient Devices – As the Commission recognized in Order No. 791, transient devices are potential vehicles for cyber-attacks absent appropriate controls.[18] To improve the defense-in-depth approach of the CIP Reliability Standards, the proposed Reliability Standards include specific requirements applicable to transient devices to further mitigate the security risks associated with such devices. Specifically, proposed Reliability Standard CIP-010-2, Requirement R4 requires entities to implement controls to protect transient devices connected to their high impact and medium impact BES Cyber Systems and associated PCAs. Responsible entities must implement controls to accomplish the following security objectives:

- prevent unauthorized access to and use of transient devices;
- mitigate the risk of vulnerabilities associated with unpatched software on transient devices; and

[18] Order No. 791 at PP 134-135.

- mitigate the risk of the introduction of malicious code on transient devices.

Similar to the framework established for protecting low impact BES Cyber Systems, responsible entities have the flexibility to determine the controls necessary to meet these security objectives. By articulating the clear security objectives described above, however, the ERO and the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity. Additionally, proposed Reliability Standard CIP-004-6, Requirement R2, Part 2.1 requires entities to provide training on the risks associated with transient devices.

Under the proposed Reliability Standards, transient devices are classified as either "Transient Cyber Assets" or "Removable Media" depending on their functionality. The terms "Transient Cyber Assets" and "Removable Media" are proposed terms for inclusion in the NERC Glossary that define the types of transient devices subject to the CIP Reliability Standards. The term "Transient Cyber Assets" refers to those programmable electronic devices, such as laptops, that are not otherwise included in a BES Cyber System or categorized as PCAs and that are used to connect on a temporary basis (i.e., 30 calendar days or less) to BES Cyber Assets, networks within an Electronic Security Perimeter ("ESP"), or PCAs for purposes such as data transfer, vulnerability assessment, maintenance, or troubleshooting. The term "Removable Media" refers to storage media that are nonprogrammable and used to connect on a temporary basis to BES Cyber Assets, networks within an ESP, or PCAs for purposes such as storing, copying, moving, or accessing data. The requirements applicable to Transient Cyber Assets and Removable Media are tailored to the capabilities of those devices.

Protection of Communication Networks – The proposed Reliability Standards also enhance the protections mandated by the CIP Version 5 Standards by requiring entities to implement security controls for nonprogrammable components of communication networks at

Control Centers with high or medium impact BES Cyber Systems. Specifically, Reliability Standard CIP-006-6, Requirement R1, Part 1.10 requires responsible entities to protect cabling and other nonprogrammable communication components (e.g., unmanaged switches, hubs, patch panels, media converters, port savers, and couplers) that are used to connect applicable Cyber Assets within the same ESP but are located outside of a Physical Security Perimeter ("PSP"). Entities must either (1) restrict physical access to such nonprogrammable communication components, or (2) implement data encryption, circuit monitoring, or equally effective protections. These protections will reduce the likelihood that "man-in-the-middle" attacks could compromise the integrity of BES Cyber Assets or PCAs at Control Centers with high or medium impact BES Cyber Systems.

Additionally, the applicability of proposed Reliability Standard CIP-007-6, Requirement R1, Part 1.2, which requires entities to protect against the use of unnecessary physical input/output ports, now includes PCAs and nonprogrammable communications components associated with high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers. Extending the scope of Part 1.2 to include PCAs and certain nonprogrammable communication components will strengthen the defense-in-depth approach provided by the CIP Reliability Standards by further minimizing the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

For the reasons discussed herein, NERC respectfully requests that the Commission approve the proposed Reliability Standards as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[19]

Charles A. Berardesco*
Senior Vice President and General Counsel
Holly A. Hawkins*
Associate General Counsel
Shamai Elstein*
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charles.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Valerie Agnew*
Director of Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
valerie.agnew@nerc.net

III. BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[20] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) 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.[21] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[22] Section 39.5(a) of the Commission's regulations requires the ERO to file for Commission approval

[19] Persons to be included on the Commission's service list are identified by an asterisk. NERC respectfully requests a waiver of Rule 203 of the Commission's regulations, 18 C.F.R. § 385.203 (2013), to allow the inclusion of more than two persons on the service list in this proceeding.

[20] 16 U.S.C. § 824o (2006).

[21] *Id.* § 824(b)(1).

[22] *Id.* § 824o(d)(5).

each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.[23]

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA and Section 39.5(c) of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.[24]

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standards were developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[25] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[26] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability Standards. The development process is open to any person or entity with a legitimate interest in

---

[23] 18 C.F.R. § 39.5(a) (2012).

[24] 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

[25] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672 at P 334, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[26] The NERC Rules of Procedure are available at http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx. The NERC Standard Processes Manual is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders. Further, a vote of stakeholders and adoption by the NERC Board is required before NERC submits the Reliability Standard to the Commission for approval.

C. Development of the Proposed Reliability Standards

As further described in Exhibit F hereto, following the issuance of Order No. 791, NERC initiated a standard development project, Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions ("Project 2014-02"), to address the following directives from Order No. 791: (1) modify or remove the "identify, assess, and correct" language in 17 requirements in the CIP Version 5 Standards; (2) develop modifications to the CIP Version 5 Standards to address security controls for low impact BES Cyber Systems; (3) develop requirements that protect transient devices; and (4) create a definition of "communication networks" and develop new or modified standards that address the protection of nonprogrammable components of communication networks.

In January 2014, the NERC Standards Committee approved a Standard Authorization Request to initiate Project 2014-02 and appointed a standard drafting team. Prior to the first meeting of the standard drafting team, NERC hosted two technical conferences in Atlanta, Georgia (January 21, 2014) and Phoenix, Arizona (January 23, 2014) to discuss the Order No. 791 directives and obtain early feedback from industry participants on possible approaches for revising the CIP Version 5 Standards to respond to the Commission's four directives.

On June 2, 2014, NERC posted the proposed Reliability Standards addressing all four directives for an initial 45-day comment period and ballot. Each of the posted Reliability Standards included revisions to address the "identify, assess, and correct" directive. Proposed Reliability Standards CIP-006-6 and CIP-007-6 also included revisions to address the communication

networks directive, and proposed Reliability Standard CIP-003-6 included revisions to address the low impact directive. The transient devices directive was addressed primarily in proposed Reliability Standard CIP-010-2, but the standard drafting team also made minor revisions in CIP-004-6, CIP-007-6, and CIP-011-2 to address this directive. On initial ballot, proposed Reliability Standards CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, and CIP-011-2 received the requisite stakeholder approval. The proposed Reliability Standards that primarily addressed the low impact and transient devices directives (CIP-003-6 and CIP-010-2), however, did not receive the requisite stakeholder approval.

The standard drafting team addressed industry comments on the initial drafts of the proposed Reliability Standards, and, on September 3, 2014, NERC posted second drafts of proposed Reliability Standards CIP-003-6 and CIP-010-2 for an additional 45-day comment period and ballot. In addition, to ensure that NERC could satisfy its regulatory deadline, NERC posted for a 45-day comment period and ballot versions of Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 that only addressed the "identify, assess, and correct" and communication networks directives.[27] All of the proposed Reliability Standards received the requisite stakeholder approval on the second posting.

After reviewing industry comment on the second drafts of the proposed Reliability Standards, however, the standard drafting team determined that additional modifications to Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 were necessary to address industry comments on the modifications related to the low impact and transient devices directives. To ensure that it could meet its regulatory deadline, on October 28,

[27] Reliability Standards CIP-006-6 and CIP-009-6 were not posted for an additional ballot because the standards did not previously include any revisions related to the low impact or transient device directives. Further, based on stakeholder comments, the standard drafting team did not identify the need for any further revisions to those standards.

2014, NERC posted for final ballot the versions of the proposed Reliability Standards that only addressed the "identify, assess, and correct" and communication networks directives. These final ballots resulted in the requisite stakeholder approvals (between 83.84% and 95.40%), and the NERC Board adopted these versions of the proposed Reliability Standards on November 13, 2014.

On November 25, 2014, after the standard drafting team addressed industry comment, NERC posted revised versions of proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 for an additional 45-day comment period and ballot to replace the versions of those Reliability Standards adopted by the Board on November 13, 2014. These additional ballots received the requisite stakeholder approval (between 81.92% and 98.89%) and, after receiving the requisite stakeholder approval in final ballots, the Board adopted the revised versions of proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-007-6, CIP-010-2, and CIP-011-2 on February 12, 2015.[28]

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standards satisfy the Commission's criteria in Order No. 672 and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The following section provides an explanation of the manner in which the proposed Reliability Standards address each of the Order No. 791 directives.

[28] During development, these revised versions of the proposed Reliability Standards were posted as CIP-003-7, CIP-004-7, CIP-007-7, CIP-10-3, and CIP-011-3 to help differentiate the revised versions from the versions adopted by the Board in November 2014. For purposes of Board adoption and filing with applicable governmental authorities, however, the version numbers are presented as -6 and -2 because the versions adopted by the Board in November 2014 were never filed with applicable governmental authorities.

A. Identify, Assess, and Correct Language

i. Order No. 791 Directive

As noted above, there are 17 requirements in the CIP Version 5 Standards that require responsible entities to implement cybersecurity policies or processes in a manner that "identifies, assesses, and corrects deficiencies." The purpose of including the "identify, assess, and correct" language was to move away from a "zero tolerance" compliance and enforcement approach and focus responsible entities on developing strong internal controls to identify and minimize instances of noncompliance. In short, the standard drafting team for the CIP Version 5 Standards recognized that while registered entities should identify, control, and minimize instances of noncompliance with those 17 requirements, it was not reasonable to expect that registered entities will be able to prevent all instances of noncompliance given the breadth and high frequency of the cybersecurity obligations therein. Further, the CIP Version 5 standard drafting team determined that it is possible that individual instances of noncompliance with those 17 requirements would be unlikely to pose a more-than-minimal risk to reliability, particularly where the responsible entity identifies the noncompliance and takes corrective action.

The CIP Version 5 standard drafting team thus concluded that, under these circumstances, the compliance and enforcement process would better promote the goals of reliability through a risk-based model, focusing industry and ERO efforts and resources on improving internal controls and avoiding instances of noncompliance that pose a more-than-minimal risk to reliability. The "identify, assess, and correct" language was intended to recognize the positive benefit to reliability of those responsible entities that have strong cultures of compliance and are proactive in their approach to identify and correct instances of noncompliance.

In Order No. 791, the Commission supported NERC's move away from a "zero tolerance" approach to compliance and the development of standards that encourage entities to improve

internal controls and focus on the activities that have the greatest impact on Bulk-Power System reliability. The Commission expressed concern, however, that the "identify, assess, and correct" language is overly vague and lacking the basic definition and guidance that is needed, for example, to distinguish a successful internal control program from one that is inadequate.[29] As such, the Commission directed NERC to remove or modify that language within one year of the date of Order No. 791. The Commission emphasized its preference for NERC to remove the language from the CIP Version 5 Standards and address the concerns underlying the "identify, assess, correct" language outside of the text of the Reliability Standards.[30] The Commission stated:

> We would prefer approaches that would not involve the placement of compliance language within the text of the Reliability Standards to address these issues. We understand that NERC has inserted the "identify, assess, and correct" language into the CIP Reliability Standard requirements to move its compliance processes towards a more risk-based model. With this objective in mind, we believe that a more appropriate balance might be struck to address the underlying concerns by developing compliance and enforcement processes that would grant NERC and the Regional Entities the ability to decline to pursue low risk violations of the Reliability Standards. Striking this balance could be accomplished through a modification to the Compliance Monitoring and Enforcement Program. We believe that such an approach would: (1) empower NERC and the Regional Entities to implement risk-based compliance monitoring techniques that avoid zero defect enforcement when appropriate; (2) allow the Commission to retain oversight over the enforcement of Reliability Standards; and (3) ensure that all Reliability Standards are drafted to be sufficiently clear and enforceable.[31]

ii. Proposed Modifications

Consistent with Order No. 791, NERC has modified the CIP Version 5 Standards by removing the "identify, assess, and correct" language from the 17 requirements that included such language.[32] NERC is addressing the concerns underlying the inclusion of the "identify, assess,

---

[29] Order No. 791 at PP 4, 67-76.

[30] *Id*. at PP 73-76.

[31] *Id*. at P 75.

[32] Each of the proposed Reliability Standards had at least one requirements with the "identify, assess and correct" language. Specifically, as noted above, the 17 requirements that included such language are: CIP-003-5,

and correct" language outside the text of a Reliability Standard through transformation of its CMEP and the implementation of a risk-based approach to compliance monitoring and enforcement activities.

In 2012, NERC launched RAI, a collaborative effort among NERC, the Regional Entities, and industry to identify and implement changes to enhance the effectiveness of the CMEP. Based on its compliance monitoring and enforcement experience, the ERO determined that a risk-based approach is essential for a proper allocation of ERO and industry resources and encourages registered entities to enhance internal controls, including those regarding the self-identification of potential noncompliance. NERC's experience indicated that a one-size-fits-all and "zero tolerance" approach to compliance monitoring and enforcement does not properly allocate time, attention, and resources to higher-risk instances of noncompliance or demonstrably equate to more reliable operations of the Bulk-Power System. It is not practical, effective, or sustainable to monitor and treat all compliance issues to the same degree or in the same manner regardless of risk and entity management practices.[33] Compliance monitoring and enforcement must be "right-sized" based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of potential noncompliance. To that end, as discussed in greater detail in the RAI Informational Filing, the RAI program involved the testing, through various pilot programs, of a number of concepts,

Requirements R2 and R4; CIP-004-5.1, Requirements R2, R3, R4, and R5; CIP-006-5, Requirements R1 and R2; CIP-007-5, Requirements R1, R2, R3, R4, and R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

[33] For instance, for high frequency security obligations, entities with effective internal controls are likely to find and correct more deficiencies than those entities without a developed approach to compliance. By treating all instances of noncompliance alike, a "zero tolerance" approach would fail to recognize and properly incentivize the development of robust internal control pursuant to which an entity is likely to identify more instances of noncompliance.

processes, and programs to develop a risk-based compliance monitoring and enforcement framework that incentivizes registered entities to develop robust compliance programs.

As a result of RAI, NERC developed a risk-based CMEP that incorporates the fundamental rationale and principles of the "identify, assess, and correct" language.[34] In general, NERC's new approach to compliance monitoring and enforcement:

- Tailors NERC's compliance monitoring and enforcement activities to the risks presented by the registered entity and the risks that the particular Reliability Standard (and/or requirement) under consideration is designed to mitigate;
- Recognizes that not all noncompliance requires formal enforcement action;
- Recognizes and rewards registered entities for efforts to improve internal controls and methods for the prompt self-identification and mitigation of noncompliance;
- Maintains ERO visibility into all instances of noncompliance to identify reliability risks and trends; and
- Maintains ERO oversight to identify implementation issues and opportunities for improvement.

The transformation to a risk-based CMEP involves the use of an oversight plan framework focused on identifying, prioritizing, and addressing risks to the Bulk-Power System to enable each Regional Entity to allocate resources where they are most needed and likely to be the most effective. The result is a compliance oversight plan for each individual registered entity. Specifically, under the risk-based CMEP, Regional Entities conduct inherent risk assessments ("IRAs") for the registered entities within their regions. An IRA is a review of potential risks posed by an individual registered entity to the reliability of the Bulk-Power System. An IRA considers factors such as assets, systems, geography, interconnectivity, and functions performed,

[34] Additional information regarding RAI and NERC's risk-based CMEP is available at http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

among others. The IRAs enable the Regional Entities to tailor oversight appropriately (i.e., focus their compliance monitoring activities on those areas for which the IRA shows greater risk).[35]

Following the IRA, a registered entity may elect to provide the Regional Entity information concerning the internal controls it uses to manage reliability risks. This process, known as the internal control evaluation ("ICE"), allows the Regional Entity to evaluate those internal controls to determine whether a registered entity has implemented effective internal controls that provide reasonable assurance of compliance with Reliability Standards associated with areas of risk identified through the IRA. By understanding how a registered entity manages or mitigates risks, the Regional Entity can further tailor its compliance oversight efforts.

Ultimately, the Regional Entity will determine the type and frequency of the compliance monitoring tools (i.e., off-site or on-site audits, spot checks, or self-certifications) warranted for a particular registered entity based on reliability risks, as determined through the IRA, and information about the registered entity's internal controls learned through the ICE process. The Regional Entity may conduct more resource-intensive compliance monitoring activities with respect to functions or registered entities within its region that can have the most significant impact on reliability. For functional roles or registered entities that have a lesser impact on reliability, the Regional Entity may tailor compliance monitoring approaches accordingly. The IRAs and ICEs thus directly accomplish the goal of the "identify, assess, and correct" language by focusing ERO and industry resources on those areas that pose a more-than-minimal risk to reliability and helping to improve internal controls.

[35] For example, a Regional Entity may choose not to include in the scope of its monitoring activities certain standards or requirements if the IRA shows less risk to reliability for those standards or requirements for that registered entity. Conversely, a Regional Entity may choose to focus its monitoring on areas for which the IRA shows greater risk.

More significantly, the risk-based CMEP also accomplishes the goal of the "identify, assess, and correct" language of moving away from a "zero tolerance" approach by allowing entities to address lower-risk instances of noncompliance outside of a formal enforcement process. Specifically, NERC is implementing (1) a compliance exception program, and (2) a self-logging program. These programs, as discussed in greater detail in the RAI informational filing, leverage existing internal practices at registered entities relating to self-monitoring, identification, assessment, and correction of noncompliance with Reliability Standards. By appropriately valuing and rewarding such efforts (i.e., by providing a disposition path outside of a formal enforcement action), the ERO encourages the enhancement of internal controls and self-identification of noncompliance throughout the industry, consistent with the intent of the "identify, assess, and correct" language. These risk-based programs apply to all Reliability Standards and requirements, not just the 17 CIP Version 5 requirements containing the "identify, assess, and correct" language.

Since 2013, the ERO has exercised discretion when deciding whether to initiate an enforcement action for noncompliance posing a minimal risk to the reliability of the BPS. Issues resolved outside of an enforcement action are referred to as compliance exceptions. Compliance exceptions reflect the "identify, assess, and correct" tenet that not all noncompliance requires processing in a formal enforcement action. Compliance exception treatment is especially appropriate if the registered entity adequately identifies its noncompliance, assesses the risk properly as minimal risk, and corrects (i.e., mitigates) the noncompliance in a timely and appropriate manner. A robust internal compliance program and management practices that led to timely discovery and timely mitigation of noncompliance may support compliance exception treatment. All minimal risk noncompliance, however, is eligible for a compliance exception regardless of discovery method.

Compliance exceptions are similar to issues remediated through the Find, Fix, Track, and Report ("FFT") program in that entities will not incur any financial penalties for issues granted a compliance exception. Compliance exceptions are not subject to formal enforcement processes. Further, a compliance exception is part of a registered entity's compliance history only to the extent that it serves to inform the ERO of potential risk. Compliance exceptions are not part of a registered entity's violation history for purposes of aggravation of penalties. Finally, to maintain visibility and allow for appropriate oversight, all compliance exceptions must be documented, submitted to NERC for review, and reported to FERC.

The self-logging program allows select registered entities with demonstrated effective internal control practices to log minimal risk noncompliance that would otherwise be individually self-reported. The registered entity must submit the log to its Regional Entity on a periodic basis for review of whether the registered entity has adequately identified and described the noncompliance, accurately assessed the risk, and appropriately mitigated the noncompliance. Once the review process is complete, the minimal risk issue is resolved as a compliance exception absent additional risk factors or other issues.

The experience of the ERO to date has shown that logs increase visibility into noncompliance detected and corrected by the registered entity, as registered entities are more likely to record instances of noncompliance on their logs than self-report them to the ERO. Further, the program fosters efficiency and reduces certain formal administrative processes associated with individual Self-Reports, allowing entities to focus more resources on protecting Bulk-Power System reliability than on administrative compliance processes.

The self-logging program is consistent with the "identify, assess, and correct" tenet that noncompliance that is self-identified through internal controls, corrected through a strong

compliance culture, and documented by the registered entity should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the Bulk-Power Systems. The risk-based enforcement processes are superior to the "identify, assess, and correct" language because they inform the Regional Entities, NERC, and FERC about the deficiencies registered entities may experience in complying with NERC's Reliability Standards. This information offers more timely feedback to Regional Entities on the effectiveness of the programs the registered entities have established for compliance with NERC's Reliability Standards.

NERC and the standard drafting team thus determined that the most appropriate response to the directive in Order No. 791 was to remove the "identify, assess, and correct" language from the CIP Reliability Standards and apply the risk-based CMEP to all of the CIP Reliability Standards. Attachment H hereto provides further information regarding the application of the risk-based CMEP to the CIP Reliability Standards.

B. Security Controls for Low Impact BES Cyber Systems

i. Order No. 791

The CIP Version 5 Standards require responsible entities to identify and categorize BES Cyber Systems using a new methodology based on whether a BES Cyber System has a low, medium, or high impact on the reliable operation of the Bulk Electric System.[36] As the Commission recognized, categorizing BES Cyber Systems in this manner, with all BES Cyber Systems categorized as at least low impact, offers more comprehensive protection of the Bulk Electric System.[37] The adoption of the low impact category will expand the protections offered

[36] *See* Reliability Standard CIP-002-5.1.

[37] Order No. 791 at P 107.

by the CIP Version 5 Standards to additional devices that, if compromised, could adversely affect the reliable operation of the Bulk Electric System.

Under the CIP Version 5 Standards, once a responsible entity identifies and categorizes a BES Cyber System under Reliability Standard CIP-002-5.1, the entity must comply with the requirements included in Reliability Standards CIP-003 to CIP-011 corresponding to the BES Cyber System's impact category. As the Commission noted, however, the only requirement in the CIP Version 5 Standards applicable to low impact BES Cyber Systems is Reliability Standard CIP-003-5, Requirement R2, which provides:

> 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:
>
> 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.

In Order No. 791, the Commission expressed concern that the CIP Version 5 Standards do not require specific controls for assets containing low impact BES Cyber Systems nor do they contain objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities under Reliability Standard CIP-003-5, Requirement R2.[38] The Commission stated that the lack of specific controls or objective criteria "introduces an unacceptable level of ambiguity and potential inconsistency into the compliance process, and creates an unnecessary gap in reliability." The Commission stated that "[t]his ambiguity will make it difficult for registered

[38] Order No. 791 at P 107.

entities to develop, and NERC and the regions to objectively evaluate, the effectiveness of procedures developed to implement Reliability Standard CIP-003-5, Requirement R2."[39] The Commission thus directed NERC to develop modifications to CIP Version 5 Standards to address this concern.

The Commission stated that NERC could address this concern in a number of ways, including:

1. requiring specific controls for low impact assets, including subdividing the assets into different categories with different defined controls applicable to each subcategory;

2. developing objective criteria against which the controls adopted by responsible entities can be compared and measured in order to evaluate their adequacy, including subdividing the assets into different categories with different defined control objectives applicable to each subcategory;

3. defining with greater specificity the processes that responsible entities must have for low impact facilities under Reliability Standard CIP-003-5, Requirement R2; or

4. another equally efficient and effective solution.[40]

ii. Proposed Modifications

To address the Commission's concern regarding the protections for low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6 includes additional specificity regarding the controls that responsible entities must implement for protecting their low impact BES Cyber Systems. As described below, proposed Reliability Standard CIP-003-6, Requirement R2 requires entities to implement controls necessary to meet specific security objectives with respect to four subject matter areas: (1) cybersecurity awareness, (2) physical security controls, (3) electronic access controls, and (4) Cyber Security Incident response. These four subject matter areas are those that were previously included in Reliability Standard CIP-003-5, Requirement R2 and that

[39] Order No. 791 at P 108.

[40] *Id*. at P 108.

the standard drafting team identified as necessary to address the risks associated with low impact BES Cyber Systems. Proposed Reliability Standard CIP-003-6, Requirement R1 also requires responsible entities to develop cybersecurity policies applicable to their low impact BES Cyber Systems to communicate management's expectations for cybersecurity across the organization.

The underlying principle of the CIP Version 5 Standards and the categorization of BES Cyber Assets as high, medium, or low impact is to require responsible entities to protect their BES Cyber Systems commensurate with the risks they present to the reliable operation of the Bulk Electric System (i.e., commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the Bulk Electric System). The goal is to focus industry resources on those areas that provide the most reliability benefit. As the Commission recognized in determining that an inventory of low impact BES Cyber Systems should not be required, given their lower risk profile, the requirements applicable to low impact BES Cyber Systems should not be overly burdensome to divert resources away from the protection of medium and high impact BES Cyber Systems.[41]

Consistent with that framework, the standard drafting team sought to develop requirements for low impact BES Cyber Systems that help mitigate the risks associated with those systems while also ensuring that responsible entities could continue to devote the necessary resources to protect their high and medium impact BES Cyber Systems. Accordingly, in contrast to the requirements applicable to high and medium impact BES Cyber Systems, the requirements applicable to low impact BES Cyber Systems may be implemented at the asset level (i.e., the protections would be applied to the site or location, such as Control Centers, Transmission stations or substations, and Generation plants, identified according to Reliability Standard CIP-002-5.1 that contain one or

[41] Order No. 791 at P 111.

more low impact BES Cyber Systems, not necessarily each BES Cyber Asset at those sites). If the low impact requirements were required to be applied at the device level, responsible entities would essentially be required to develop an inventory of low impact BES Cyber Systems, undercutting the goal of focusing industry resources on those areas that provide the greatest benefits to reliability.

Further, the standard drafting team concluded that focusing on the four subject matter areas listed above will have the greatest cybersecurity benefit for low impact BES Cyber Systems without diverting resources necessary for the protection of high and medium impact BES Cyber Systems. As discussed below, requiring entities to: (1) regularly reinforce cybersecurity awareness and best practices across the organization; (2) establish protections to control physical access; (3) establish electronic access controls to limit inbound and outbound communication; and (4) implement Cyber Security Incident response plans will help mitigate the risk and impact of cyber-attacks targeting low impact BES Cyber Systems.

Considering the large number and diversity of low impact BES Cyber Systems, proposed Reliability Standard CIP-003-6, Requirement R2 provides responsible entities the flexibility to implement security controls for low impact BES Cyber Systems in the manner that best suits the needs and characteristics of their organization, so long as the responsible entity can demonstrate that it designed its controls to meet the ultimate security objectives. The standard drafting team concluded that attempts to overly prescribe specific controls for low impact BES Cyber Systems would be problematic given the diversity of low impact BES Cyber Systems and likely inhibit the development of innovative security controls. By articulating clear security objectives, however, the ERO and the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity.

Reliability Standard CIP-003-6, Requirement R2 provides that "[e]ach Responsible Entity with at least one asset identified in CIP-002-5.1 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that includes the sections in Attachment 1" to the proposed Reliability Standard. Attachment 1 provides as follows:

> Responsible Entities shall include each of the sections provided below in the cyber security plan(s) required under Requirement R2.
>
> Responsible Entities with multiple-impact BES Cyber Systems ratings can utilize policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plan(s). Each Responsible Entity can develop a cyber security plan(s) either by individual asset or groups of assets.
>
> Section 1. Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).
>
> Section 2. Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset and (2) the Low Impact BES Cyber System Electronic Access Points (LEAPs), if any.
>
> Section 3. Electronic Access Controls: Each Responsible Entity shall:
>
> 3.1 For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access; and
>
> 3.2 Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability.
>
> Section 4. Cyber Security Incident Response: Each Responsible Entity shall have one or more Cyber Security Incident response plan(s), either by asset or group of assets, which shall include:
>
> 4.1 Identification, classification, and response to Cyber Security Incidents;
>
> 4.2 Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and

subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law;

4.3 Identification of the roles and responsibilities for Cyber Security Incident response by groups or individuals;

4.4 Incident handling for Cyber Security Incidents;

4.5 Testing the Cyber Security Incident response plan(s) at least once every 36 calendar months by: (1) responding to an actual Reportable Cyber Security Incident; (2) using a drill or tabletop exercise of a Reportable Cyber Security Incident; or (3) using an operational exercise of a Reportable Cyber Security Incident; and

4.6 Updating the Cyber Security Incident response plan(s), if needed, within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.

The protections required by Requirement R2, Attachment 1 reflect the level of risk that misuse or the unavailability of low impact BES Cyber Systems poses to the BES. The following is a discussion of each section in Attachment 1:

Section 1 requires responsible entities to develop and implement a plan to reinforce good cybersecurity practices within their organization. The standard drafting team found that regular communication emphasizing cybersecurity practices can significantly improve an entity's cybersecurity posture. To that end, Section 1 requires responsible entities to take measures to reinforce cybersecurity practices at least once every 15 months. The responsible entity has the discretion to determine the topics to be addressed and the manner in which it will communicate these topics, so long as the responsible entity can demonstrate that its reinforcement activities are designed to raise cybersecurity awareness and promote a culture of security. The topics can include the physical security of BES Cyber Systems as well as technology-specific topics.

Section 2 addresses the physical security of low impact BES Cyber Systems, requiring responsible entities to document and implement methods to control physical access to: (1) low impact BES Cyber Systems; and (2) Low Impact BES Cyber System Electronic Access Points (or LEAPs), if any. A LEAP, which is a proposed term for inclusion in the NERC Glossary, is essentially an interface that controls electronic access to an asset containing a low impact BES Cyber System or the low impact BES Cyber System. A LEAP is defined as:

> A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems.

The term Low Impact External Routable Connectivity (or LERC), which is also a proposed term for inclusion in the NERC Glossary, is defined as

> Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols).[42]

The responsible entity has the discretion to select the method used to control physical access based on organizational need. As discussed in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-003-6, the responsible entity may use one or a combination of access controls, monitoring controls, or other operational, procedural, or technical physical security controls. Entities may use facility-level perimeter controls (e.g., fences with locked gates, guards, or site access policies, etc.) or set up controls in the specific areas where low impact BES

[42] The exclusion of point-to-point communications between intelligent electronic devices was included so as not to inhibit the functionality of the time-sensitive requirements related to this technology nor to preclude the use of such time-sensitive reliability enhancing functions if they use a routable protocol in the future.

Cyber Systems are located, such as control rooms or control houses. The controls to be implemented are necessarily dependent on the type of facility in question (e.g., limiting physical access to BES Cyber Systems at a wind generating facility spread across many acres of land requires a different set of controls than those required at a Transmission station). Regardless of the method chosen or the types of assets to be protected, the physical access controls must be designed to meet the overall security objective of limiting physical access to those individuals that need to be in a particular location to carry out the functions of the organization, whether it be a system operator or a vendor that needs to service a particular device.

Section 3 requires responsible entities to establish electronic boundary protections for low impact BES Cyber Systems that have bi-directional routable protocol communication with, or Dial-up Connectivity to, devices external to the asset containing the low impact BES Cyber Systems. The boundary protections are intended to control communication either into the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System to reduce the risks associated with uncontrolled communication using routable protocols or Dial-up Connectivity. Considering the wide array of low impact BES Cyber Systems and the risk-based approach to protecting different types of BES Cyber Systems, the standard drafting team focused the electronic access controls on access external to the asset containing the low impact BES Cyber System and not on inter-asset communication. From a risk perspective, controlling the accessibility to or from the asset containing the low impact BES Cyber System significantly reduces the scale of threats to low impact BES Cyber Systems.

Pursuant to Section 3, if there is LERC, then a responsible entity must implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access. The

Guidelines and Technical Basis section of the proposed Reliability Standard describes situations where LERC exists:

> …LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to, logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session, even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bi-directional routable communication from or to the low impact BES Cyber System.

The Guidelines and Technical Basis section also provides examples of electronic access controls that would meet the security objectives, such as implementing a LEAP with explicitly defined inbound and outbound access permissions or using a host-based firewall to control the inbound and outbound access between the low impact BES Cyber System and the Cyber Asset in an external network.[43] Fundamentally, the goal is to ensure that low impact BES Cyber Systems are adequately separated from general purpose business networks and not accessible from the internet.

Responsible entities have flexibility in the method they use to control electronic access. As described in the Guidelines and Technical Basis section, in selecting an interface to control LERC (i.e., the LEAP), entities could use, for example, (1) the internal (facing the low impact BES Cyber Systems) interface on an external or host-based firewall, (2) the internal interface on a router that has implemented an access control list, or (3) another security device. Responsible entities also have flexibility with respect to the location of the LEAP, which is not required to reside at the

[43] The Guidelines and Technical Basis section also provides examples of situations that would lack sufficient access controls to meet the security objective.

asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP for every asset containing low impact BES Cyber Systems. Rather, responsible entities can have a single Cyber Asset containing multiple LEAPs that control LERC for multiple assets containing low impact BES Cyber Systems. Regardless of the method chosen to implement the LEAP, responsible entities must meet the ultimate security objective of permitting only necessary inbound and outbound bi-directional routable protocol access.

Section 4 requires responsible entities to have one or more documented response plans that set forth the actions they must take when responding to a Cyber Security Incident associated with low impact BES Cyber Systems. These response plans will help ensure that entities can respond efficiently and effectively to any Cyber Security Incidents at assets containing low impact BES Cyber Systems and, in turn, limit any adverse impact. Additionally, by requiring entities to determine whether a Cyber Security Incident is a Reportable Cyber Security Incident (requiring notification to the ES-ISAC), the Cyber Security Incident response plans will help ensure that other responsible entities are aware of the incident and take appropriate action to protect their BES Cyber Systems. The Cyber Security Incident response plans do not need to be on a per asset site or per low impact BES Cyber System basis. Entities can use a single enterprise-wide plan for all low impact BES Cyber Systems.

For each of these sections, those responsible entities that have multi-impact-rated BES Cyber Systems can use the policies, procedures, and processes for their high or medium impact BES Cyber Systems to fulfill the sections for the development of low impact cyber security plans. This approach may create efficiencies for entities and allow them to better manage their resources. Moreover, in recognition of the diverse set of low impact BES Cyber Systems, responsible entities

can develop the cybersecurity plan(s) required by CIP-003-6, Requirement R2 either by individual asset or groups of assets.

In addition to the plans required by Requirement R2, proposed Reliability Standard CIP-003-6, Requirement R1, Part 1.2 retains the requirement that responsible entities develop management-approved cybersecurity policies for their assets containing low impact BES Cyber Systems. These policies must cover the same four subject matter areas (cybersecurity awareness, physical security controls, electronic access controls, and Cyber Security Incident response) and must be reviewed and approved by the CIP Senior Manager at least once every 15 calendar months. Proposed Reliability Standard CIP-003-6, Requirement R1 does not dictate the form or content of these policies. The responsible entity has the flexibility to develop a single comprehensive cybersecurity policy covering the required topics, or it may choose to develop a single high-level umbrella policy and provide additional policy detail related to the required topics in lower level documents in its documentation hierarchy. Under either scenario, however, the purpose of these policies is to communicate the responsible entity's management goals, objectives, and expectations for the protection of low impact BES Cyber Systems and establish a culture of security and compliance across the organization. These policies, together with the plans required under Requirement R2, provide a framework for implementing operational, procedural, and technical safeguards for securing low impact BES Cyber Systems commensurate with the risks they present.

C. Protection of Transient Devices

i. Order No. 791

In Order No. 791, the Commission directed NERC to modify the CIP Version 5 Standards to develop requirements that protect transient devices (e.g., thumb drives and laptop computers)

that fall outside the definition of BES Cyber Asset.[44] The FERC-approved definition of BES Cyber Asset provides, in relevant part:

> 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.

The purpose of the 30-day exemption is to exclude transient devices from the full suite of cyber security protections applicable to BES Cyber Assets in the CIP Version 5 Standards. As the Commission agreed in Order No. 791, given that transient devices are portable and frequently connected and disconnected from systems, it would be unduly burdensome to protect transient devices in the same manner as BES Cyber Assets.[45]

Nevertheless, the Commission expressed concern as to whether the CIP Version 5 Standards provide adequately robust protection from the risks posed by transient devices, such as the introduction of malicious code. While the Commission acknowledged that the CIP Version 5 Standards already require that entities protect their BES Cyber Systems from malicious code, no matter the source, the Commission stated that "relying on a single security control to protect information systems is contrary to the fundamental cyber security concept of defense-in-depth." The Commission thus directed NERC to modify the CIP Version 5 Standards to addresses the risks posed by transient devices.

The Commission stated that the requirements should recognize that transient devices, unlike BES Cyber Assets, are generally portable and frequently connected and disconnected from systems. The Commission also "expects NERC to consider the following security elements when designing a Reliability Standard for transient devices: (1) device authorization as it relates to users

---

[44] Order No. 791 at PP 132-36.

[45] *Id*. at P 133.

and locations; (2) software authorization; (3) security patch management; (4) malware prevention; (5) detection controls for unauthorized physical access to a transient device; and (6) processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact)."

ii. Proposed Modifications

Consistent with Order No. 791 and to improve the defense-in-depth protections of the CIP Reliability Standards, the proposed Reliability Standards include specific requirements to mitigate the risks associated with transient devices. As most BES Cyber Systems are already isolated from external public or untrusted networks pursuant to the CIP Version 5 Standards, the use of transient devices is a potential vehicle for cyber-attacks. As the Commission recognized, "transient devices have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations" and, because these devices can move between ESPs, they could spread malware across a responsible entity's various BES Cyber Systems absent appropriate controls.[46] Using transient devices, however, is often the only way for responsible entities to transport files to and from secure areas to maintain, monitor, or troubleshoot BES Cyber Systems.

Accordingly, as described further below, NERC revised its CIP Reliability Standards, consistent with Order No. 791, to require entities to: (1) develop plans and implement cybersecurity controls to protect Transient Cyber Assets and Removable Media associated with their high impact and medium impact BES Cyber Systems and associated PCAs (CIP-010-2, Requirement R4); and (2) train their personnel on the risks associated with using Transient Cyber Assets and Removable Media (CIP-004-6, Requirement R2, Part 2.1). The purpose of the proposed revisions is to: (1) prevent unauthorized access to and the use of transient devices; (2)

[46] Order No. 791 at P 135.

mitigate the risk of vulnerabilities associated with unpatched software on such devices; and (3) mitigate the risk of the introduction of malicious code on such devices.

The standard drafting team determined that applying the proposed requirements to transient devices associated with high and medium impact BES Cyber Systems will help ensure that responsible entities appropriately focus their resources on protecting those BES Cyber Systems that, if compromised, present the greatest risks to reliability and warrant the defense-in-depth protections discussed in Order No. 791. The standard drafting team concluded that the application of the proposed transient devices requirements to transient devices associated with low impact BES Cyber Systems was unnecessary, and likely counterproductive, given the risks low impact BES Cyber Systems present to the Bulk Electric System. As discussed above, the standard drafting team sought to develop requirements for low impact BES Cyber Systems that mitigate the risks associated with those systems while ensuring that industry could still devote the necessary resources to protecting medium and high impact BES Cyber Systems. Applying the proposed transient devices requirements to low impact BES Cyber Systems could divert resources away from protecting medium and high BES Cyber Systems.

To manage risks associated with the use of Transient Cyber Assets and Removable Media across impact levels, however, the standard drafting team explicitly required responsible entities to implement the security controls before connecting such devices to high and medium impact BES Cyber Systems and their associated PCAs. As such, if a responsible entity uses the same Transient Cyber Assets and Removable Media across all impact levels, the risks posed by these devices are mitigated at all impact levels.

The following is a discussion of the proposed definitions associated with the proposed requirements applicable to transient devices and a description of those requirements.

a. Proposed Definitions Related to Transient Devices

To define and clarify the types of transient devices subject to the CIP Reliability Standards, NERC is proposing to add the following two terms to the NERC Glossary: (1) Transient Cyber Asset, and (2) Removable Media. The proposed definition of Transient Cyber Asset is:

> A Cyber Asset that (i) is capable of transmitting or transferring executable code, (ii) is not included in a BES Cyber System, (iii) is not a Protected Cyber Asset (PCA), and (iv) is directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless, including near field or Bluetooth communication) for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a PCA. Examples include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Examples of Transient Cyber Assets include, but are not limited to, diagnostic test equipment, packet sniffers, equipment used for BES Cyber System maintenance, equipment used for BES Cyber System configuration, or equipment used to perform vulnerability assessments. Transient Cyber Assets can be one of many types of devices, including a specially-designed device for maintaining equipment in support of the Bulk Electric System or a platform, such as a laptop, desktop, or tablet computer, which interfaces with or runs applications that support BES Cyber Systems.

The proposed definition of Removable Media is:

> Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

The standard drafting team also revised the definitions for BES Cyber Asset and PCA to remove the 30-day exemption. The proposed definition of Transient Cyber Asset obviates the need for the 30-day exemption as it covers those Cyber Assets that would otherwise have been subject to the 30-day exemption and specifically states that a Transient Cyber Asset is not included

in a BES Cyber System and is not a PCA. As defined, Transient Cyber Assets and Removable Media do not provide reliability services and are not part of the BES Cyber System to which they are connected.

b. Proposed Requirements Applicable to Transient Cyber Assets and Removable Media

To protect BES Cyber Systems from the risks associated with transient devices, proposed Reliability Standard CIP-010-2, Requirement R4 requires entities to document and implement a plan for managing and protecting Transient Cyber Assets and Removable Media. Specifically, Requirement R4 provides that "[e]ach responsible entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, [to] implement, except under CIP Exceptional Circumstances, one or more documented plans for Transient Cyber Assets and Removable Media that include the sections in Attachment 1" to the proposed Reliability Standard. Attachment 1 sets forth the content that responsible entities must include in their plan(s). As described below, Attachment 1 does not prescribe a standard method or set of controls that each entity must implement to protect its transient devices. Instead, Attachment 1 requires responsible entities to meet certain security objectives by implementing the controls that the responsible entity determines necessary to meet its affirmative obligation to protect its transient devices. This approach provides the responsible entity the flexibility to implement the controls that best suit the needs and characteristics of its organization. To comply with Requirement R4, however, the responsible entity must be able to demonstrate that its selected controls were designed to meet the ultimate security objectives outlined in Attachment 1.

Under Attachment 1, responsible entities' plans must address the following three areas:

1. Protections for Transient Cyber Assets managed by the Responsible Entity.
2. Protections for Transient Cyber Assets managed by a party other than the Responsible Entity (e.g., vendors or contractors).

3. Protections for Removable Media.

These three sections reflect the standard drafting team's recognition that the security controls required for a particular transient device must account for the functionality of that device and/or whether the responsible entity or a third party manages the device. Because Transient Cyber Assets and Removable Media have different capabilities, they present different levels of risk to the Bulk Electric System, and the protections required under the proposed Reliability Standards must reflect those differences. For instance, Transient Cyber Assets are subject to vulnerabilities associated with unpatched software, while Removable Media are not. Similarly, the standard drafting team recognized that because a responsible entity lacks complete control over Transient Cyber Assets managed by a third party, it cannot implement the procedures for those devices (e.g., the responsible entity has limited authority to patch software on a device owned and managed by a third party).[47] The responsible entity, however, still has the responsibility to mitigate the risks associated with Transient Cyber Assets managed by a third party prior to connection. Accordingly, the standard drafting team established different requirements for Transient Cyber Assets managed by the responsible entity and those managed by a third-party, as well as for Removable Media.[48]

The following is a discussion of the security objectives and/or protections applicable to each of these sections:

Transient Cyber Assets Managed by the Responsible Entity: Attachment 1 provides as follows regarding Transient Cyber Assets managed by the responsible entity:

Section 1. Transient Cyber Asset(s) Managed by the Responsible Entity.

---

[47] Many responsible entities rely on third-party vendors or contractors to provide support services to BES Cyber Systems.

[48] Given the functionality of Removable Media, the standard drafting team concluded that it was not necessary to distinguish between Removable Media managed by the responsible entity and those managed by a third party. That is because, no matter who manages Removable Media, the same type of security controls can be applied (e.g., the scanning of a thumb drive prior to connection).

1.1. Transient Cyber Asset Management: Responsible Entities shall manage Transient Cyber Asset(s), individually or by group: (1) in an ongoing manner to ensure compliance with applicable requirements at all times, (2) in an on-demand manner applying the applicable requirements before connection to a BES Cyber System, or (3) a combination of both (1) and (2) above.

1.2. Transient Cyber Asset Authorization: For each individual or group of Transient Cyber Asset(s), each Responsible Entity shall authorize:

1.2.1. Users, either individually or by group or role;

1.2.2. Locations, either individually or by group; and

1.2.3. Uses, which shall be limited to what is necessary to perform business functions.

1.3. Software Vulnerability Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):

- Security patching, including manual or managed updates;
- Live operating system and software executable only from read-only media;
- System hardening; or
- Other method(s) to mitigate software vulnerabilities.

1.4. Introduction of Malicious Code Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the introduction of malicious code (per Transient Cyber Asset capability):

- Antivirus software, including manual or managed updates of signatures or patterns;
- Application whitelisting; or
- Other method(s) to mitigate the introduction of malicious code.

1.5. Unauthorized Use Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of unauthorized use of Transient Cyber Asset(s):

- Restrict physical access;
- Full-disk encryption with authentication;
- Multi-factor authentication; or
- Other method(s) to mitigate the risk of unauthorized use.

Section 1.1 requires responsible entities to document how they plan to manage their Transient Cyber Assets. While responsible entities have the flexibility to manage their Transient

Cyber Assets on a continuous basis or on an as-needed basis, requiring entities to document how they are managing Transient Cyber Assets will help ensure that applicable personnel understand the steps they need to take prior to using a particular Transient Cyber Asset. Such documentation will thus help reduce the likelihood that a Transient Cyber Asset will be connected to a BES Cyber Asset, a network within an ESP, or a PCA absent the proper protections.

Section 1.2 requires entities to limit the use of their Transient Cyber Assets to a specific set of authorized users, locations, and business functions. For authorizing users, responsible entities may authorize by individual, department, or specific job function. Similarly, when authorizing locations, the entity may specify a discrete location or a group of locations. Lastly, when authorizing uses for an individual or group of Transient Cyber Assets, the entity may specify one or more business functions or tasks for which the device may be used. As part of this process, the entity should also specify any software or application packages authorized to be included on the device that are necessary to perform the specified business function or task (e.g., data transfer, vulnerability assessment, maintenance, or troubleshooting) as well as the authorized network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections).

By controlling who may use a Transient Cyber Asset, and where and for what purpose that Transient Cyber Asset may be used, entities will reduce the chances that Transient Cyber Assets could spread malware across their BES Cyber Systems. For example, if an entity restricts the use of certain laptop computers to Control Centers with high impact BES Cyber Systems and only includes software and applications on the laptop computer used for troubleshooting purposes, the entity not only limits the opportunity for that laptop computer to be the vehicle for a cyber-attack but also limits the potential impact if it were to be used as a vehicle in a cyber-attack.

Section 1.3 creates an affirmative obligation on each responsible entity to take the necessary steps to mitigate the risk of vulnerabilities posed by unpatched software on its Transient Cyber Assets. Entities must use one or more of the following methods to achieve this security objective: (1) security patching, including manual or managed updates;[49] (2) live operating system and software executable only from read-only media;[50] (3) system hardening;[51] or (4) other methods that are equally as effective at mitigating software vulnerabilities. While entities have significant flexibility to choose whatever method best suits their needs, regardless of the method(s) chosen, each responsible entity must be able to demonstrate that it used appropriate methods to meet its affirmative obligation to mitigate software vulnerabilities on its Transient Cyber Assets.

The phrase "per Transient Cyber Asset capability" is used in Section 1.3 and elsewhere in Attachment 1 to clarify that if a particular mitigation method cannot be implemented for a particular Transient Cyber Asset, an entity is not required to use that particular method. Nevertheless, the entity continues to be responsible for implementing an equally effective method, if necessary and capable, to meet the ultimate security objective.

Section 1.4 obligates entities to document and implement processes to mitigate the risk of introducing malicious code into a BES Cyber System through a Transient Cyber Asset. Entities must use one or more of the following methods to achieve this security objective: (1) antivirus

---

[49] The responsible entity has the flexibility to include its Transient Cyber Assets in its enterprise-wise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset.

[50] This method will help mitigate software vulnerabilities by creating protected operating systems that cannot be modified to deliver malicious software.

[51] System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function.

software, including manual or managed updates of signatures or patterns;[52] (2) application whitelisting;[53] or (3) other equally effective methods. While entities have the flexibility to choose whatever method best suits their needs, each responsible entity must be able to demonstrate that it used appropriate methods to meet its affirmative obligation to mitigate the risks of introducing malicious code. When addressing malicious code protection, the responsible entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered on a Transient Cyber Asset, it must be removed or mitigated to prevent it from being introduced into a BES Cyber Asset or BES Cyber System.

Lastly, Section 1.5 requires entities to document and implement processes for mitigating the risk of unauthorized use of Transient Cyber Assets. If there is an unauthorized use of a Transient Cyber Asset, there is an increased risk that the device could be tampered with or exposed to malware. Entities must use one or more of the following methods to achieve the security objective of mitigating the risk of unauthorized use: (1) restrict physical access; (2) full-disk encryption with authentication; (3) multi-factor authentication; or (4) other equally effective methods.[54] Again, regardless of the method(s) chosen, each responsible entity must be able to demonstrate that it used appropriate methods to meet its affirmative obligation to mitigate the risks of unauthorized use.

---

[52] Entities have the flexibility to deploy antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns, or scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

[53] Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.

[54] Additional information on each of these methods is provided in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-010-2.

Transient Cyber Assets Managed by a Third Party: Responsible entities often use third-party vendors and contractors to provide support services to BES Cyber Systems. The third-party vendors or contractors frequently use Transient Cyber Assets to provide such services. As such, the standard drafting team recognized that to mitigate the risks associated with the use of Transient Cyber Assets, it was also necessary to require entities to take steps to protect their BES Cyber Systems from the risks associated with using Transient Cyber Assets managed by a third party. Because responsible entities have less control over those devices, the standard drafting team recognized that the requirements applicable to such devices must account for that lack of control.[55] Accordingly, the requirements related to such devices are in a separate section and focus on reviewing the third party's controls and taking any necessary follow-up action if the entity deems such controls insufficient to mitigate the risks associated with such devices. Specifically, Attachment 1 provides the following for Transient Cyber Assets managed by a third party:

> **Section 2.** Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.
>
> **2.1** Software Vulnerabilities Mitigation: Use one or a combination of the following methods to achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset (per Transient Cyber Asset capability):
>
> - Review of installed security patch(es);
> - Review of security patching process used by the party;
> - Review of other vulnerability mitigation performed by the party; or
> - Other method(s) to mitigate software vulnerabilities.
>
> **2.2** Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):
>
> - Review of antivirus update level;
> - Review of antivirus update process used by the party;

[55] For instance, the responsible entity cannot limit the users of the device, the locations at which the device is used, or the purposes for which the device is used.

- Review of application whitelisting used by the party;
- Review use of live operating system and software executable only from read-only media;
- Review of system hardening used by the party; or
- Other method(s) to mitigate malicious code.

2.3 For any method used to mitigate software vulnerabilities or malicious code as specified in 2.1 and 2.2, Responsible Entities shall determine whether any additional mitigation actions are necessary and implement such actions prior to connecting the Transient Cyber Asset.

Sections 2.1 and 2.2 have the same security objective as Sections 1.3 and 1.4, respectively, requiring responsible entities take the necessary steps to mitigate software vulnerabilities on Transient Cyber Assets and the introduction of malicious code. Because Sections 2.1 and 2.2 address devices managed by a third party, however, the focus is on reviewing the security controls used by the third party to ensure there are sufficient protections in place. Following the entity's review under Sections 2.1 and 2.2, Section 2.3 requires the entity to determine whether any additional actions are necessary to mitigate the risks associated with using a third party's Transient Cyber Asset. If additional actions are necessary, the entity must take such actions prior to connecting the Transient Cyber Asset to an applicable system. Regardless of the method(s) and/or actions the entity chooses to implement under Section 2, the entity must be able to demonstrate that it used appropriate methods to meet the overall security objective.

Removable Media: Although, as noted above, Removable Media do not have the same functionality as Transient Cyber Assets, the standard drafting team recognized that such devices can be the source of a cyber-attack and must be protected. For instance, while Removable Media are not subject to software vulnerabilities, it is possible for such devices to spread malware. As the Commission pointed out in Order No. 791, there were "two recent situations where malware was introduced into electric generation industrial control systems (ICS) through removable media

(i.e. a USB drive) that was being used to back-up a control system environment and updates."[56] Accordingly, under Section 3 of Attachment 1, entities are required to document and implement processes for: (1) limiting who may use Removable Media and at what locations; and (2) mitigating the threat of introducing malicious code to high or medium impact BES Cyber Systems and their associated PCAs. Specifically, Section 3 of Attachment 1 provides as follows:

> **Section 3.** Removable Media
>
> **3.1** Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:
>
> **3.1.1.** Users, either individually or by group or role; and
>
> **3.1.2.** Locations, either individually or by group.
>
> **3.2.** Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:
>
> **3.2.1.** Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and
>
> **3.2.2.** Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

Section 3.1 requires entities to limit the use of Removable Media to a specific set of authorized users and locations. When authorizing users, responsible entities may authorize by individual, department, or specific job function. Similarly, when authorizing locations, the entity may specify a discrete location or a group of locations.[57] By controlling who may use Removable Media and where Removable Media may be used, entities will reduce the chances that Removable Media could spread malware across their BES Cyber Systems.

---

[56] Order No. 791 at n.166.

[57] Given the limited functionality of Removable Media, as compared to Transient Cyber Assets, the standard drafting team concluded that it was unnecessary to require responsible entities to limit the uses of Removable Media as well.

Similar to Sections 1.4 and 2.2, discussed above, Section 3.2 requires entities to take the necessary steps to mitigate the risk of introducing malicious code into a BES Cyber System through Removable Media. Sections 3.2.1 and 3.2.2 create an affirmative obligation to (1) use methods to detect malicious code on Removable Media, and (2) mitigate the threat of any detected malicious code on Removable Media before connecting the device to a high impact or medium impact BES Cyber System or associated PCA. In implementing methods to detect malicious code, entities must use a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. Regardless of the methods chosen to detect and mitigate malicious code, the responsible entity must demonstrate that it used appropriate methods to meet the overall security objective of mitigating the risks of introducing malicious code through Removable Media.

In addition to the protections required by Reliability Standard CIP-010-2, Requirement R4, proposed Reliability Standard CIP-004-6, Requirement R2, Part 2.1 requires entities to provide training on the risks associated with Transient Cyber Assets and Removable Media. Specifically, Part 2.1 provides that entities must provide training on "[c]yber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and Removable Media." This training will help reinforce the protections required by proposed Reliability Standard CIP-010-2, Requirement R4.

D. Protection of Communication Networks

i. Order No. 791

In Order No. 791, the Commission approved the revised definition for the term "Cyber Asset," which removed reference to "communication networks."[58] The Commission concluded

[58] Order No. 791 at P 148. The currently-effective NERC Glossary definition of Cyber Asset is "[p]rogrammable electronic devices and communication networks including hardware, software, and data." The

that: (1) "it is not necessary to maintain the phrase 'communications network' within the text of the Cyber Asset definition to ensure that the programmable electronic components of these networks receive protection under the CIP Reliability Standards;" and (2) "maintaining the phrase "communication networks" within the Cyber Asset definition would likely cause confusion and possibly complicate the implementation of the CIP version 5 Standards, as many communication network components, such as cabling, cannot strictly comply with the CIP Reliability Standards."[59]

The Commission expressed concern, however, that the CIP Version 5 Standards do not explicitly address security controls needed to protect the nonprogrammable components of communication networks.[60] The Commission directed NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the protection of the nonprogrammable component of communication networks within one year of the date of Order No. 791.[61] The Commission stated that (1) the definition of communication networks should define what equipment and components should be protected, and (2) the new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks.

ii. Proposed Modifications

As the Commission has recognized, if entities do not take steps to secure nonprogrammable components of communication networks used to connect BES Cyber Assets, those components

definition of Cyber Asset approved in Order No. 791 is "[p]rogrammable electronic devices, including the hardware, software, and data in those devices."

59 Order No. 791 at P 148.

60 *Id*. at P 149. The Commission noted that other information security standards address the protection of communication mediums, for instance in NIST SP 800-53 Rev. 3, security control PE-4 includes examples of protecting communication medium including: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

61 *Id*. at P 150.

could be used to access BES Cyber Assets and ultimately compromise the reliable operation of the Bulk-Power System.[62] To address this concern, the proposed Reliability Standards require entities to implement security controls for nonprogrammable components of communication networks (e.g., cabling, wiring, unmanaged switches, hubs, patch panels, media converters, port savers, and couplers) at Control Centers with high or medium impact BES Cyber Systems. The standard drafting team focused on nonprogrammable communication components at Control Centers with high or medium impact BES Cyber Systems because those locations present a heightened risk to the Bulk-Power System warranting the increased protections. As discussed above, the CIP Reliability Standards are designed to focus industry resources on protecting those BES Cyber Systems and associated devices or communication mediums that present increased risks to the reliable operation of the Bulk Electric System.

Proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 provides that, for high impact BES Cyber Systems and their associated PCAs, and medium impact BES Cyber Systems at Control Centers and their associated PCAs, responsible entities must either physically secure nonprogrammable communication components that are located outside a PSP (e.g., by conduit, secured cable trays, or secured communication closets) or implement other effective protections (e.g., data encryption or circuit monitoring) to mitigate the risks associated with exposed nonprogrammable communication components. Specifically, Part 1.10 provides that responsible entities must take the following action:

> Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter.

[62] Order No. 791 at PP 148-149; *North American Electric Reliability Corporation*, 142 FERC ¶ 61,203 (2013).

Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following:

- encryption of data that transits such cabling and components;
- monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or
- an equally effective logical protection.

The protections required by Part 1.10 will reduce the possibility of tampering and the likelihood that "man-in-the-middle" attacks could compromise the integrity of BES Cyber Systems or PCAs at Control Centers with high or medium impact BES Cyber Systems. For example, responsible entities will now be required to protect cabling between a data center and a control room where the Cyber Assets in the data center and control room are in the same ESP but the cabling is outside a PSP. Proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 applies only to nonprogrammable components outside of a PSP because nonprogrammable components located within a PSP are already subject to physical security protections by virtue of being within a PSP. Reliability Standard CIP-006-6, Requirements R1, R2, and R3 require entities to implement various security controls to restrict and manage physical access to PSPs.

Similarly, Part 1.10 only applies to nonprogrammable components used for connection between applicable Cyber Assets within the same ESP because Reliability Standard CIP-005-5 already requires logical protections for communications between discrete ESPs. For instance, under CIP-005-5, Requirement R2 responsible entities must do the following for Interactive Remote Access into an ESP: (1) use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset; (2) use encryption

that terminates at an Intermediate System; and (3) require multi-factor authentication for all Interactive Remote Access sessions.

Responsible entities have the discretion as to the type of physical or logical protections to implement pursuant to CIP-006-6, Requirement R1, Part 1.10, provided that the protections are designed to meet the overall security objective. The standard drafting team provided this flexibility to allow entities to implement the physical security measure(s) that best suits their needs and to account for configurations where logical measures are necessary because the entity cannot implement physical access restrictions effectively. As the Commission has recognized, where physical security protections for communication mediums cannot be implemented effectively, logical measures may be an appropriate alternative to accomplishing the security objective.[63]

If the entity chooses to implement physical security measures, the entity must design such measures to effectively restrict physical access to the nonprogrammable communication components, such as the use of a padlock on a communications closet, armored cabling, or stainless steel or aluminum tube protecting the fiber inside an optical ground wire cable.[64] Regardless of the specific control(s) implemented, the entity must physically protect the entirety of the nonprogrammable communication component, including any termination points that may be outside of a defined PSP. Similarly, if an entity chooses to implement logical protections, the entity must design such measures to effectively mitigate the risks associated with exposed communication components.

---

63 *North American Electric Reliability Corporation*, 132 FERC ¶ 61,051 (2010).

64 As discussed in the Guidelines and Technical Basis section of the proposed Reliability Standard, these physical security measures should be implemented in such a way that they would provide some mechanism to detect or recognize that someone could have tampered with the cabling or other nonprogrammable components.

Additionally, proposed Reliability Standard CIP-007-6, Requirement R1, Part 1.2 extends the requirement for entities to protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media to PCAs and nonprogrammable communications components associated with all high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers.[65] Pursuant to the proposed modification, the network ports included in the scope of Part 1.2 are not limited to those on the BES Cyber System itself but also include ports that exist on PCAs and nonprogrammable communication components, such as unmanaged switches, hubs, or patch panels, located within a PSP and an ESP. The extended applicability of Part 1.2 will strengthen the defense-in-depth approach provided by the CIP Reliability Standards by further minimizing the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.[66]

The proposed modification to Part 1.2 applies to nonprogrammable communication components within a PSP and an ESP for applicable BES Cyber Systems to allow for a scenario where the responsible entity implements an extended ESP covering multiple locations (with corresponding logical protections identified in CIP-006-6, Requirement R1, Part 1.10). The standard drafting team limited the applicability in this manner to clarify that responsible entities are not responsible for protecting nonprogrammable communication components outside of the responsible entity's control (i.e., components of a telecommunication carrier's network).

Finally, the standard drafting team concluded that it was not necessary to develop a definition of the phrase "communication network" to address the Commission's concerns

---

[65] The extension of Part 1.2 to PCAs and nonprogrammable communication components is consistent with NIST SP 800-53 Rev. 3, security control PE-4.

[66] The standard drafting team also revised Part 1.2 to capitalize the term "Removable Media."

regarding the protection of nonprogrammable components of communication networks. As the Commission recognized in its order remanding a proposed interpretation of Reliability Standard CIP-006-4, the term "communication network" is generally understood to encompass both programmable components and nonprogrammable components (i.e., a communication network includes computers peripherals, terminals, and databases as well as communication mediums such as wires).[67] In turn, any proposed definition would need to be sufficiently broad to encompass all components in a communication network as they exist now and in the future.[68] Rather than trying to circumscribe the exact components of a communication network in a NERC Glossary definition, the standard drafting team simply identified the types of equipment or components that entities must protect and proposed appropriate and reasonable controls to secure those components based on the risks they present to the Bulk Electric System.

The standard drafting team did not identify the need to use a broadly-defined term in the CIP Reliability Standards to accomplish the security objective to protect nonprogrammable communication components. Whether or not there is a NERC Glossary definition for the term "communication network," NERC's cybersecurity standards, as proposed, meet the ultimate security objective of protecting communication networks (both programmable and nonprogrammable communication network components). First, the CIP Version 5 Standards already include protections for programmable components of a communication network as BES Cyber Assets or PCAs, depending on their function and location. In addition, the proposed Reliability Standards include protections for cables and other the nonprogrammable

---

67 *North American Electric Reliability Corporation*, 142 FERC ¶ 61,203 at PP 13-14 (2013).

68 For example, NIST Special Publication 800-53, Revision 4 refers to the CNSSI 4009 definition of Network, which is "[i]nformation system(s) implemented with a collection of interconnected components."

communication components, as discussed above, to augment the existing protections for programmable communication components.

E. Enforceability of the Proposed Reliability Standards

The proposed Reliability Standards include VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standards. The VRFs and VSLs for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment. Exhibit E provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

The proposed Reliability Standards also include measures that support each requirement by clearly identifying what is required and how the ERO will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[69]

V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standards to become effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan is designed to match the effective dates of the proposed Reliability Standards with the effective dates of the prior versions of those Reliability Standards under the implementation plan for the CIP Version 5 Standards (the "CIP V5 Implementation Plan"), provided that responsible entities have at least three months to implement the proposed Reliability Standards. The purpose of this approach is to provide responsible entities regulatory certainty by limiting the time, if any, that the CIP Version 5 Standards with the

[69] Order No. 672 at P 327.

"identify, assess, and correct" language would be effective.[70] Specifically, pursuant to the CIP V5 Implementation Plan, the effective date of each of the CIP Version 5 Standards is April 1, 2016, except that the effective date for Requirement R2 of CIP-003-5, which addresses protections for low impact BES Cyber Systems, is April 1, 2017. Consistent with those dates, the proposed Implementation Plan provides that: (1) each of the proposed Reliability Standards "shall become effective on the later of April 1, 2016 or the first day of the first calendar quarter that is three calendar months after" the effective date of the Commission's order approving the proposed Reliability Standard; and (2) responsible entities will not have to comply with the proposed requirements applicable to low impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) until April 1, 2017.

Where the standard drafting team identified the need for additional time for implementation of a particular section of a proposed Reliability Standard (i.e., an entire Requirement or a portion thereof), however, the proposed Implementation Plan provides additional time for compliance with that particular section. Specifically, the standard drafting team provided additional implementation time for those sections of the proposed Reliability Standards that create entirely new obligations (as opposed to simply removing or slightly modifying an existing obligation) that require responsible entities to develop new processes and procedures and devote substantial resources for implementation. Because those new obligations were not anticipated when the effective dates for the CIP Version 5 Standards were established, the standard drafting team concluded that additional time was necessary to ensure an effective and efficient implementation of both the existing obligations in the CIP Version 5 Standards and the revisions proposed herein.

[70] If the timing of the Commission's order approving the proposed Reliability Standards results in the CIP Version 5 Standards with the "identify, assess, and correct" language taking effect, NERC would not enforce the "identify, assess, and correct" provisions during the short time that those standards would be effective.

The compliance dates for those particular sections of the proposed Reliability Standards represent the dates that entities must begin to comply with those sections, even where the Reliability Standards go into effect at an earlier date.

The following is a description of the compliance dates for each of the sections in the proposed Reliability Standards where the standard drafting team identified the need for additional time for implementation:

- *Reliability Standard CIP-003-6, Requirement R1, Part 1.2* – Entities are not required to comply with Part 1.2 until the later of April 1, 2017 or nine calendar months after the effective date of CIP-003-6. This additional time is consistent with the implementation period provided in the CIP V5 Implementation Plan for obligations related to low impact BES Cyber Systems.

- *Reliability Standard CIP-003-6, Requirement R2* - Entities are not required to comply with Requirement R2 until the later of April 1, 2017 or nine calendar months after the effective date of CIP-003-6. This additional time is consistent with the implementation period provided in the CIP V5 Implementation Plan for CIP-003-5, Requirement R2. Additionally, entities are not required to comply with Sections 2 and 3 of Attachment 1 to Reliability Standard CIP-003-6 until the later of September 1, 2018 or nine calendar months after the effective date of CIP-003-6. The standard drafting team concluded that an additional 17 months was necessary to ensure an effective implementation of the controls required by Section 2 and 3 of Attachment 1.

- *Reliability Standard CIP-006-6, Requirement R1, Part 1.10* – For new high or medium impact BES Cyber Systems at Control Centers which were not identified as Critical Cyber Assets under the currently effective version of the CIP Reliability Standards, responsible entities are not required to comply with Part 1.10 until nine calendar months after the effective date of Reliability Standard CIP-006-6. Because entities were already protecting nonprogrammable components of communication networks under the currently effective version of the CIP Reliability Standards, the additional time for compliance with Part 1.10 only applies to communication components associated with newly identified BES Cyber Systems.

- *Reliability Standard CIP-007-6, Requirement R1, Part 1.2* – Responsible entities are not required to comply with Part 1.2 for their applicable PCAs and nonprogrammable communication components until nine calendar months after the effective date of Reliability Standard CIP-007-6. The standard drafting team concluded that an additional nine months was an appropriate time frame for compliance with the new obligations.

- *Reliability Standard CIP-010-2, Requirement R4* – Responsible entities are not required to comply with Requirement R4 until nine calendar months after the effective date of Reliability Standard CIP-010-2. The standard drafting team concluded that an additional

nine months was an appropriate time frame for compliance with the new obligations associated with transient devices as entities will have to develop and implement new plans and processes to ensure effective compliance.

As to the proposed new and modified definitions, the Implementation Plan provides that their effective dates correspond to the compliance dates for those sections of the proposed Reliability Standards in which they are used. Specifically, the new and modified definitions associated with the transient devices directive (i.e., BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset) shall become effective on the compliance date for Reliability Standard CIP-010-2, Requirement R4. Similarly, the new and modified definitions associated with the low impact directive (i.e., Low Impact BES Cyber System Electronic Access Point and Low Impact External Routable Connectivity) shall become effective on the compliance date for Reliability Standard CIP-003-6, Requirement R2.

Lastly, the Implementation Plan provides that the retirement of Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1 shall become effective on the effective date of the proposed Reliability Standards.

VI. CONCLUSION

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

- the proposed Reliability Standards and associated elements included in Exhibit A, effective as proposed herein;
- the proposed Implementation Plan included in Exhibit B;
- the proposed new and revised definitions to be incorporated into the NERC Glossary included in Exhibit A; and
- the retirement of Commission-approved Reliability Standards CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-1, and CIP-011-1, effective as proposed herein.

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charles.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 13, 2015