152 FERC ¶ 61,054
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM15-14-000]

Revised Critical Infrastructure Protection Reliability Standards

(July 16, 2015)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to approve seven critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). The North American Electric Reliability Corporation (NERC) submitted the proposed Reliability Standards in response to the Commission's Order No. 791. The proposed Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition, the Commission proposes to direct NERC to develop certain modifications to Reliability Standard CIP-006-6 and to develop requirements addressing supply chain management.

DATES: Comments are due **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:

- Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

Instructions: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:

Daniel Phillips (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6387
daniel.phillips@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
kevin.ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

152 FERC ¶ 61,054
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standards — Docket No. RM15-14-000

NOTICE OF PROPOSED RULEMAKING

(July 16, 2015)

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission proposes to approve seven critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). The North American Electric Reliability Corporation, the Commission-certified Electric Reliability Organization (ERO), submitted the proposed Reliability Standards in response to Order No. 791.[2] The Commission also proposes to approve NERC's proposed implementation plan and violation risk factor and violation severity level assignments. In addition, we propose to approve NERC's proposed new or revised definitions for inclusion in the NERC Glossary of Terms Used in Reliability

[1] 16 U.S.C. 824o.

[2] *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 reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

Standards (NERC Glossary). Further, the Commission proposes to approve 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.

2. The proposed Reliability Standards are designed 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 cybersecurity incident, would affect the reliable operation of the Bulk-Power System.[3] As discussed below, we believe that the proposed CIP Reliability Standards are just and reasonable and address the directives in Order No. 791 by: (1) eliminating the "identify, assess, and correct" language in 17 of the CIP version 5 Standard requirements; (2) providing enhanced security controls for Low Impact assets; (3) providing controls to address the risks posed by transient electronic devices (e.g., thumb drives and laptop computers); and (4) addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication networks." Accordingly, we propose to approve the proposed CIP Reliability Standards because they improve the base-line cybersecurity posture of applicable entities compared to the current Commission-approved CIP Reliability Standards.

3. In addition, pursuant to FPA section 215(d)(5), the Commission proposes to direct NERC to develop certain modifications to Reliability Standard CIP-006-6. Specifically,

[3] *See* NERC Petition at 3.

while proposed CIP-006-6 would require protections for communication networks among a limited group of bulk electric system Control Centers, we propose to direct that NERC modify Reliability Standard CIP-006-6 to require protections for communication network components and data communicated between all bulk electric system Control Centers. In addition, we seek comment on the sufficiency of the security controls incorporated in the current CIP Reliability Standards regarding remote access used in relation to bulk electric system communications. Finally, as discussed in more detail below, we propose to direct NERC to develop requirements relating to supply chain management for industrial control system hardware, software, and services.

I. Background

A. Section 215 and Mandatory Reliability Standards

4. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[4] Pursuant to section 215 of the FPA, the

[4] 16 U.S.C. 824o(e).

Commission established a process to select and certify an ERO,[5] and subsequently certified NERC.[6]

B. Order No. 791

5. On November 22, 2013, in Order No. 791, the Commission approved the CIP version 5 Standards (Reliability Standards CIP-002-5 through CIP-009-5, and CIP-010-1 and CIP-011-1).[7] The Commission determined that the CIP version 5 Standards represented an improvement over prior iterations of the CIP Reliability Standards because, *inter alia*, they included a revised BES Cyber Asset categorization methodology that incorporated mandatory protections for all High, Medium, and Low Impact BES Cyber Assets, and because several new security controls improved the security posture of responsible entities.[8] In addition, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC to: (1) remove the "identify, assess, and correct" language in 17 of the CIP Standard requirements; (2) develop enhanced security controls for Low Impact assets; (3) develop controls to protect transient electronic devices (e.g., thumb drives and laptop computers); (4) create a NERC Glossary definition for the term

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

[6] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[7] Order No. 791, 145 FERC ¶ 61,160 at P 41.

[8] *Id.*

"communication networks," and develop new or modified Reliability Standards to protect the nonprogrammable components of communications networks.

6. In addition, the Commission directed NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition and submit an informational filing within one year.[9] Finally, the NOPR directed Commission staff to convene a technical conference to examine the technical issues concerning communication security, remote access, and the National Institute of Standards and Technology (NIST) Risk Management Framework.[10]

C. Informational Filing

7. On February 3, 2015, NERC submitted an informational filing assessing the results of a survey conducted to identify the scope of assets subject to the definition of the term BES Cyber Asset as it is applied in the CIP version 5 Standards. NERC states that the results of the survey indicate that, in general, the application of the BES Cyber Asset definition, and the 15 minute parameter in particular, resulted in the identification of BES Cyber Assets consistent with the language and intent of the CIP version 5 Standards.[11] NERC maintained that the survey results demonstrate that the definition of BES Cyber

[9] *Id.* PP 76, 108, 136, 150.

[10] *Id.* P 225.

[11] *See* NERC Informational Filing, Docket No. RM13-5-000, at 3 (filed Feb. 3, 2015).

Asset provides a sound basis for identifying the types of Cyber Assets that should be subject to the cyber security protections required by the CIP Reliability Standards.[12]

D. April 29, 2014 Technical Conference

8. On April 29, 2014, a staff-led technical conference was held pursuant to a directive in Order No. 791.[13] The topics discussed at the technical conference included: (1) the adequacy of the approved CIP version 5 Standards' protections for Bulk-Power System data being transmitted over data networks; (2) whether additional security controls are needed to protect Bulk-Power System communications networks, including remote systems access; and (3) the functional differences between the respective methods utilized for the identification, categorization, and specification of appropriate levels of protection for cyber assets using the CIP version 5 Standards as compared with those employed within the NIST Cybersecurity Framework.

9. With respect to the current state of protection for communications networks under the CIP version 5 Standards, some panelists opined that the CIP version 5 Standards lack controls to: (1) protect communications outside of the Electronic Security Perimeter; (2) protect data in motion; (3) authenticate messages and commands to BES Cyber Assets; and (4) protect systems or communications using non routable protocols. On the subject of the adequacy of protections for Bulk-Power System data under the CIP version 5 Standards, several panelists stated that stronger measures, such as encryption,

[12] *Id.*

[13] Order No. 791, 145 FERC ¶ 61,160 at P 225.

would enhance the overall protection for Bulk-Power System communications. However, other panelists also stated that encryption was not a universal solution because it could cause unacceptable latency (i.e., time delay in communications) in certain applications.

10. Regarding the need for additional security controls for Bulk-Power System communications, panelists identified a number of worthwhile steps that could be explored to enhance remote access. Suggestions included the adoption of additional physical security controls, integrity checks, encryption (in certain cases), out of bounds detection for communications links, and coordination with vendors to enhance risk management. In addition, certain panelists stated their position that the use of intermediate systems, alone, is not sufficient to address remote access concerns.[14] Several panelists identified suggestions that could be explored to enhance protections for remote access, including the addition of logical or physical controls to provide additional network segmentation behind the intermediate systems.[15]

E. NERC Petition

11. On February 13, 2015, NERC submitted a petition seeking approval of Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and

[14] An Intermediate System is defined as "A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter." NERC Glossary at 46 (April 29, 2015).

[15] *See* Transcript at pp. 176-177 (Kevin Perry speaking), 177-178 (Richard Kinas speaking), 178 (Dr. Andrew Wright speaking), 179 (Andrew Ginter speaking).

CIP-011-2, as well as the proposed implementation plan,[16] associated violation risk factor and violation severity level assignments, proposed new or revised definitions,[17] and 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.[18] NERC states that the proposed Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest because they satisfy the factors set forth in Order No. 672 that the Commission applies when reviewing a proposed Reliability Standard.[19] NERC maintains that the proposed Reliability Standards "improve the cybersecurity protections required by the CIP Reliability Standards[.]"[20]

12. NERC avers that the proposed CIP Reliability Standards satisfy the Commission directives in Order No. 791. Specifically, NERC states that the proposed Reliability Standards remove the "identify, assess, and correct" language, which represents the

[16] 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 of the CIP version 5 Standards.

[17] The six new or revised definitions proposed for inclusion in the NERC Glossary are: (1) BES Cyber Asset; (2) Protected Cyber Asset; (3) Low Impact Electronic Access Point; (4) Low Impact External Routable Connectivity; (5) Removable Media; and (6) Transient Cyber Asset.

[18] The proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM15-14-000 and on the NERC website, www.nerc.com.

[19] *See* NERC Petition at 13 and Exhibit C (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 323-335).

[20] NERC Petition at 4.

Commission's preferred approach to addressing the underlying directive.[21] In addition, NERC states that the proposed Reliability Standards address the Commission's directive regarding a lack of specific controls or objective criteria for Low Impact BES Cyber Systems by requiring responsible entities "to implement cybersecurity plans for assets containing Low Impact BES Cyber Systems to meet specific security objectives relating to: (i) cybersecurity awareness; (ii) physical security controls; (iii) electronic access controls; and (iv) Cyber Security Incident response."[22]

13. With regard to the Commission's directive that NERC develop specific controls to protect transient electronic devices (e.g., thumb drives and laptop computers), NERC explains that the proposed Reliability Standards require responsible entities "to implement controls to protect transient devices connected to their high impact and medium impact BES Cyber Systems and associated [Protected Cyber Assets]."[23] In addition, NERC states that the proposed Reliability Standards address the protection of communication networks "by requiring entities to implement security controls for nonprogrammable components of communication networks at Control Centers with high or medium impact BES Cyber Systems."[24] Finally, NERC explains that it has not proposed a definition of the term "communication network" because the term is not used

[21] *Id.* at 4, 15.

[22] *Id.* at 5.

[23] *Id.* at 6.

[24] *Id.* at 8.

in the CIP Reliability Standards. Additionally, NERC states that "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."[25] NERC concludes that the proposed Reliability Standards "meet the ultimate security objective of protecting communication networks (both programmable and nonprogrammable communication network components)."[26]

14. Accordingly, NERC requests that the Commission approve the proposed Reliability Standards, the proposed implementation plan, the associated violation risk factor and violation severity level assignments, and the proposed new and revised definitions. NERC requests an effective date for the Reliability Standards of the later of April 1, 2016 or the first day of the first calendar quarter that is three months after the effective date of the Commission's order approving the proposed Reliability Standard, although NERC proposes that responsible entities will not have to comply with the requirements applicable to Low Impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) until April 1, 2017.

II. Discussion

15. Pursuant to section 215(d)(2) of the FPA, we propose to approve Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2 as just, reasonable, not unduly discriminatory or preferential, and in the public

[25] *Id.* at 51-52.

[26] *Id.* at 52.

interest. In addition, pursuant to FPA section 215(d)(5), we propose to direct NERC to develop certain modifications to Reliability Standard CIP-006-6 and to develop requirements addressing supply chain management.

16. The proposed Reliability Standards address the Commission's directives from Order No. 791 and are an improvement over the current Commission-approved CIP Reliability Standards. Specifically, we propose to approve the removal of the "identify, assess, and correct" language in certain requirements of the CIP version 5 Standards. We also propose to approve NERC's submission regarding the protection of Low Impact BES Cyber Systems. With regard to the directive to create a NERC Glossary definition for the term "communication networks," we propose to approve NERC's proposal as an equally effective and efficient method to achieve the reliability goal underlying that directive in Order No. 791.

17. The technical controls in proposed Reliability Standard CIP-006-6, which addresses the protection of non-programmable components of communication networks (i.e., network cabling and switches), are generally consistent with the type of controls cited by the Commission in Order No. 791.[27] We are concerned, however, that the limited applicability of the proposed standard, i.e., BES Cyber Assets within the same Electronic Security Perimeter but located outside of a Physical Security Perimeter, results in a reliability gap. For the reasons discussed below, we propose to direct that NERC

[27] *See* Order No. 791, 145 FERC ¶ 61,160 at P 149.

modify Reliability Standard CIP-006-6 to require physical or logical protections for communication network components between all bulk electric system Control Centers.

18. Separately, we are concerned that changes in the bulk electric system cyber threat landscape, identified through recent malware campaigns targeting supply chain vendors, have highlighted a gap in the protections under the CIP Reliability Standards. These malware campaigns represent a new type of threat to the reliability of the bulk electric system where malicious code can infect the software of industrial control systems used by responsible entities. Therefore, we propose to direct NERC to develop a new Reliability Standard or modified Reliability Standard to provide security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations.

19. We also propose to approve the new or revised definitions for inclusion in the NERC Glossary, and seek comment on the proposed definition for Low Impact External Routable Connectivity. Depending on the comments received, we may direct NERC to develop modifications to this definition to eliminate possible ambiguities and ensure that BES Cyber Assets receive adequate protection.

20. In addition, we propose to accept 19 violation risk factor and violation severity level assignments associated with the proposed Reliability Standards. Finally, we propose to approve NERC's proposed implementation plan and effective date. Below, we discuss the following matters: (A) -identify, assess, and correct language; (B) enhanced security controls for Low Impact assets; (C) protection of Transient Devices; (D) protection of bulk electric system communication networks; (E) supply

chain management; (F) proposed definitions; (G) NERC's proposed implementation plan; and (H) proposed violation severity level and violation risk factor assignments.

A. Identify, Assess, and Correct Language

Order No. 791

21. In the proposed CIP version 5 Standards, NERC included language in 17 CIP requirements that would have required responsible entities to implement requirements in a manner to "identify, assess, and correct" deficiencies.[28] In Order No. 791, the Commission concluded that the "identify, assess, and correct" language proposed by NERC was unclear with respect to the obligations it would impose on responsible entities, how it would be implemented by responsible entities, and how it would be enforced.[29] The Commission explained that proposed Reliability Standards should be clear and unambiguous regarding what is required for compliance and who is required to comply.[30] The Commission directed NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards to address the Commission's concerns with the "identify, assess, and correct" language. The Commission stated its preference that NERC should remove the "identify, assess, and correct" language from

[28] Order No. 791, 145 FERC ¶ 61,160 at P 44.

[29] *Id.* P 67.

[30] *Id.* P 68 (citing *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 274, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007)).

the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[31]

NERC Petition

22. In its Petition, NERC explains that it has addressed the Order No. 791 directive regarding the "identify, assess, and correct" language by removing the language from the 17 requirements that included the language in the CIP version 5 Standards.[32] NERC states that it is addressing the concerns underlying the development of the "identify, assess, and correct" language through "transformation of its [Compliance Monitoring and Enforcement Program] and the implementation of a risk-based approach to compliance monitoring and enforcement activities."[33] NERC explains that the changes it is making to the Compliance Monitoring and Enforcement Program, outside the text of a reliability standard, "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."[34]

Discussion

23. NERC's proposal to remove the "identify, assess, and correct" language from the 17 requirements that included the language in the CIP version 5 Standards, while

[31] *Id.* P 67 (citing Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 186).

[32] NERC Petition at 15.

[33] *Id.* at 15-16.

[34] *Id.* at 18.

retaining the substantive provisions of those requirements, reflects the Commission's preferred approach outlined in Order No. 791.[35] Consistent with the rationale underlying the Order No. 791 directive, removing the "identify, assess, and correct" language avoids the possibility of inconsistent application and enforcement of the requirements at issue by eliminating the possibility of multiple interpretations of that language.

24. Accordingly, we propose to approve NERC's removal of the "identify, assess, and correct" language from the 17 affected requirements.

B. Enhanced Security Controls for Low Impact Assets

Order No. 791

25. In Order No. 791, the Commission approved NERC's new approach to categorizing BES Cyber Systems based on the High, Medium or Low Impact that each system could have on the reliable operation of the bulk electric system. Specifically, the Commission noted that the new tiered approach, "which requires at least a minimum classification of Low Impact for BES Cyber Systems, better assures the protection of assets that can cause cyber security risks to the bulk electric system."[36] The Commission, however, raised concerns that the CIP version 5 Standards do not require any specific controls for BES Cyber Systems classified as Low Impact, nor do the standards contain clear, objective criteria "to judge the sufficiency of the controls ultimately adopted by

[35] Order No. 791, 145 FERC ¶ 61,160 at P 67.

[36] *Id.* P 87.

responsible entities for Low Impact BES Cyber Systems."[37] The Commission concluded that the lack of objective criteria to evaluate any controls adopted under proposed Reliability Standard CIP-003-5, Requirement R2 "introduces an unacceptable level of ambiguity and potential inconsistency into the compliance process," resulting in an unnecessary gap in reliability.[38] The Commission therefore directed NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards to address the ambiguity and potential for inconsistency in the compliance process created by the lack of objective criteria pertaining to Low Impact BES Cyber Systems.[39]

26. While not directing NERC to develop specific controls for Low Impact BES Cyber Systems, the Commission noted that NERC could address the lack of objective criteria 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

[37] *Id.* P 107.

[38] *Id.* P 108.

[39] *Id.* P 108.

efficient and effective solution.[40] Finally, the Commission emphasized that however NERC decides to address the Commission's concern, "the criteria NERC proposes for evaluating a responsible entities' protections for Low Impact facilities should be clear, objective, commensurate with their impact on the system, and technically justified."[41]

NERC Petition

27. In its Petition, NERC states that the revised CIP Reliability Standards include "additional specificity regarding the controls that responsible entities must implement for protecting their low impact BES Cyber Systems."[42] NERC explains that proposed Reliability Standard CIP-003-6, Requirement R1 requires responsible entities to develop cyber security policies for Low Impact BES Cyber Systems "to communicate management's expectation for cybersecurity across the organization."[43] According to NERC, the cyber security policies required under proposed Reliability Standard CIP-003-6, Requirement R1 must include the four subject matter areas addressed by proposed Reliability Standard CIP-003-6, Requirement R2, Attachment 1, and must be reviewed and approved by the CIP Senior Manager at least once every 15 calendar months. NERC explains that, while a responsible entity has the flexibility to develop either a single comprehensive cyber security policy or single high-level umbrella policy with detail provided in lower-level documents, "the purpose of these policies is to communicate the responsible entity's management goals, objectives, and expectations for

[40] *Id.* P 108.

[41] *Id.* P 110.

the protection of low impact BES Cyber Systems and establish a culture of security and compliance across the organization."[44]

28. In addition, NERC explains that proposed Reliability Standard CIP-003-6, Requirement R2 requires responsible entities with Low Impact BES Cyber Systems to implement controls necessary to meet specific security objectives for: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) cyber security incident response. NERC explains further that while the four topics addressed by Reliability Standard CIP-003-6, Requirement R2 are the same as those under the CIP version 5 Standards, focusing resources on the four identified subject matter areas "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."[45]

29. NERC explains further that proposed Reliability Standard CIP-003-6, Requirement R2 provides responsible entities with flexibility to adopt 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

---

[42] NERC Petition at 23.

[43] *Id.* at 24.

[44] *Id.* at 32.

[45] *Id.* at 25.

it designed its controls to meet the ultimate security objective."[46] NERC states that attempts to overly prescribe specific security controls would be problematic and could inhibit the development of innovative security controls due to the diversity of Low Impact BES Cyber Systems. However, NERC explains that by having responsible entities articulate clear security objectives, "the ERO and the Commission will have a basis from which to judge the sufficiency of the controls ultimately adopted by a responsible entity."[47]

Discussion

30. We propose to approve proposed Reliability Standard CIP-003-6. NERC's proposal satisfies the Commission's Order No. 791 directive by providing responsible entities with a list of specific security objectives relevant to Low Impact BES Cyber Systems that must be addressed through one or more documented cyber security plans. Reliability Standard CIP-003-6, Requirement R2 provides clarity regarding what is expected for compliance and requires responsible entities to implement specific security controls to meet the four subject matter areas identified by NERC to address the risks associated with Low Impact BES Cyber Systems, providing enhanced protections for Low Impact assets.

31. As noted above, Attachment 1 to revised CIP-003-6, Requirement R2 identifies four topics addressed by the requirement, and describes the affirmative obligations

[46] *Id.* at 25.

[47] *Id.* at 25.

associated with each topic, including: (1) mandatory reinforcement of cyber security awareness practices at least once every 15 calendar months; (2) mandatory physical access controls to the asset or locations of the Low Impact BES Cyber Systems within the asset and Low Impact BES Cyber System Electronic Access Points, if any; (3) mandatory electronic access point protection to permit only necessary inbound and outbound bi-directional routable protocol access and mandatory authentication for all dialup connectivity that provides access to the Low Impact BES Cyber System; and (4) specific information to be included in incident response plans. We believe that Attachment 1 provides sufficient context to evaluate objectively the effectiveness of the procedures developed by a responsible entity to implement CIP-003-6 and judge the sufficiency of the controls ultimately adopted by a responsible entity under its security plans.

32. Furthermore, we agree that NERC's proposal to use clear security objectives in lieu of specific security controls for each Low Impact system is reasonable owing to the diversity of assets covered under the Low Impact category. With respect to the security subject matter areas covered under proposed CIP-003-6, we believe that NERC's proposal is reasonable in relation to the risk posed by Low Impact BES Cyber Systems, as well as the diversity of systems captured by the Low Impact category. Therefore, we propose to approve proposed Reliability Standard CIP-003-6.

C. Protection of Transient Devices

Order No. 791

33. In Order No. 791, the Commission approved the proposed definition of BES Cyber Asset that provides, in part, that "[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 [Electronic Security Perimeter], a Cyber Asset within an [Electronic Security Perimeter], or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes."[48] While the Commission had requested comment in the CIP version 5 NOPR on whether the 30 consecutive calendar day qualifier in the proposed definition of BES Cyber Asset "could result in the introduction of malicious code or new attack vectors to an otherwise trusted and protected system,"[49] the Commission concluded, based on comments, that "it would be unduly burdensome to protect transient devices in the same manner as BES Cyber Assets because transient devices are portable and frequently connected and disconnected from systems."[50]

34. While accepting the 30-day exemption in the BES Cyber Asset definition, the Commission reiterated its concern whether the provisions of the CIP version 5 Standards "provide adequately robust protection from the risks posed by transient devices."[51] Therefore, the Commission directed that NERC, pursuant to section 215(d)(5) of the FPA, develop either new or modified Reliability Standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems. In particular, the Commission stated that it expects NERC to consider the following security elements

[48] Order No. 791, 145 FERC ¶ 61,160 at P 132.

[49] *Version 5 Critical Infrastructure Protection Reliability Standards*, 143 FERC ¶ 61,055, at P 78 (2013) (CIP Version 5 NOPR).

[50] Order No. 791, 145 FERC ¶ 61,160 at P 133.

[51] *Id.* P 132.

for transient devices and removable media: (1) device authorization as it relates to users 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).[52]

NERC Petition

35. In its Petition, NERC states that the revised CIP Reliability Standards satisfy the Commission's directive in Order No. 791 by requiring that applicable entities: (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 Protected Cyber Assets; and (2) train their personnel on the risks associated with using Transient Cyber Assets and Removable Media. NERC states that the purpose of the proposed revisions is to prevent unauthorized access to and use of transient devices, mitigate the risk of vulnerabilities associated with unpatched software on transient devices, and mitigate the risk of the introduction of malicious code on transient devices. NERC explains that the standard drafting team determined that the proposed requirements should only apply to transient devices associated with High and Medium Impact BES Cyber Systems, concluding that "the application of the proposed transient devices requirements to transient devices associated with low impact BES

[52] *Id.* P 136.

Cyber Systems was unnecessary, and likely counterproductive, given the risks low impact BES Cyber Systems present to the Bulk Electric System."[53]

36. NERC proposes to add two terms to the NERC Glossary, Transient Cyber Asset and Removable Media, to clarify the types of transient devices subject to the CIP Reliability Standards. NERC also proposes to revise the definitions for BES Cyber Asset and Protected Cyber Asset to remove the 30-day exemption as the proposed definition for Transient Cyber Assets obviates the need for the 30-day exemption language. NERC indicates that, 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.[54]

37. NERC proposes to define Transient Cyber Asset as: "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 [Electronic Security Perimeter], or a [Protected Cyber Asset]." NERC explains that 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

[53] NERC Petition at 34-35.

[54] *Id.* at 36-37.

used to perform vulnerability assessments, and may include devices or platforms such as laptops, desktops or tablet computers which run applications that support BES Cyber Systems.[55]

38. NERC proposes to define the term Removable Media as: "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 [Electronic Security Perimeter] 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."[56]

39. NERC explains that 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 in order to protect BES Cyber Systems from the risks associated with transient devices. Specifically, Requirement R4 provides that "[e]ach responsible entity for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall 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 standard]." NERC indicates that Attachment 1 does not prescribe a standard method or

[55] *Id.* at 36.

[56] *Id.* at 36.

set of controls that each entity must implement to protect its transient devices, but rather requires responsible entities to meet certain security objectives by implementing the controls that the responsible entity determines are necessary to meet its affirmative obligation to protect BES Cyber Systems.[57]

40. NERC further explains that Attachment 1 to CIP-010-2, Requirement R4 requires a responsible entity to adopt controls to address the following areas: (1) protections for Transient Cyber Assets managed by responsible entities; (2) protections for Transient Cyber Assets managed by another party; and (3) protections for Removable Media. NERC indicates that these provisions reflect the standard drafting team's recognition that the security controls required for a particular transient device must account for (1) the functionality of that device and (2) whether the responsible entity or a third party manages the device. NERC also states that, because Transient Cyber Assets and Removable Media have different capabilities, they present different levels of risk to the bulk electric system.[58]

Discussion

41. Based on our review, proposed Reliability Standard CIP-010-2 appears to provide a satisfactory level of security for transient devices used at High and Medium Impact BES Cyber Systems. As described above, proposed Reliability Standard CIP-010-2, Requirement R4 addresses the following security elements: (1) device authorization;

[57] *Id.* at 37.

[58] *Id.* at 38.

(2) software authorization; (3) security patch management; (4) malware prevention; and (5) unauthorized use. The proposed security controls, taken together, constitute a reasonable approach to address the reliability objectives outlined by the Commission in Order No. 791. The proposed security controls outlined in Attachment 1 should ensure that responsible entities apply multiple security controls to provide defense-in-depth protection to transient devices (i.e., transient cyber assets and removable media) in the High and Medium Impact BES Cyber System environments.

42. We are concerned, however, that NERC's proposed revisions do not provide adequate security controls to address the risks posed by transient devices used at Low Impact BES Cyber Systems, including Low Impact control centers, due to the limited applicability of Requirement R4. We believe that this omission may result in a gap in protection for Low Impact BES Cyber Systems. For example, malware inserted via a USB flash drive at a single Low Impact substation could propagate through a network of many substations without encountering a single security control under NERC's proposal. In addition, we note that Low Impact security controls do not provide for the use of mandatory anti-malware/antivirus protections within the Low Impact facilities, heightening the risk that malware or malicious code could propagate through these systems without being detected.

43. We do not believe that NERC has provided an adequate justification to limit the applicability of Reliability Standard CIP-010-2. In its petition, NERC states 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."[59] Essentially, NERC posits that resources are better placed in the protection of High and Medium Impact devices. The burden of expanding the applicability of Reliability Standard CIP-010-2 to transient devices at Low Impact BES Cyber Systems, however, is not clear from the information in the record. Nor is it clear what information and analysis led NERC to conclude that the application of the transient device requirements to Low Impact BES Cyber Systems "was unnecessary."[60] Therefore, we direct NERC to provide additional information supporting the proposed limitation in Reliability Standard CIP-010-2 to High and Medium Impact BES Cyber Systems. Depending on the information provided, we may direct NERC to address the potential reliability gap by developing a solution, which could include modifying the applicability section of CIP-010-2, Requirement R4 to include Low Impact BES Cyber Systems, that effectively addresses, and is appropriately tailored to address, the risks posed by transient devices to Low Impact BES Cyber Systems.

D. Protection of Bulk Electric System Communication Networks

Order No. 791

44. In Order No. 791, the Commission approved a revised definition of the NERC Glossary term Cyber Asset, including the removal of the phrase "communication networks." In reaching its decision, the Commission recognized that maintaining the

[59] NERC Petition at 34-35.

[60] *Id.*

phrase "communication networks" in the definition of "cyber asset" could cause confusion and potentially complicate implementation of the CIP version 5 Standards "as many communication network components, such as cabling, cannot strictly comply with the CIP Reliability Standards."[61]

45. However, while the Commission approved the revised Cyber Asset definition, the Commission also directed NERC to create a definition of communication networks. Specifically, the Commission stated that "[t]he definition of communication networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System."[62]

46. The Commission also directed NERC to develop new or modified Reliability Standards to address the reliability gap resulting from the removal of the phrase "communication networks" from the Cyber Asset definition. Specifically, the Commission found that a gap in protection may exist since the CIP version 5 Standards "do not address security controls needed to protect the nonprogrammable components of communication networks."[63] The Commission explained that the new or modified Reliability Standards should require appropriate and reasonable controls to protect the

[61] Order No. 791, 145 FERC ¶ 61,160 at P 148.

[62] *Id.* P 150.

[63] *Id.* P 149.

non-programmable aspects of communication networks.[64] The Commission provided examples of other relevant information security standards that address the protection of the nonprogrammable aspects of communication networks by requiring, among other things, locked wiring closets, disconnected or locked spare jacks, protection of cabling by conduit or cable trays, or generally emphasizing the protection of communication network cabling from interception or damage.[65]

NERC Petition

47. In its petition, NERC states that the standard drafting team concluded that it did not need to create a new definition for communication networks to address the Commission's concerns. NERC explains that the term communication network "is generally understood to encompass both programmable and nonprogrammable components (i.e., a communication network includes computer peripherals, terminals, and databases as well as communication mediums such as wires)."[66] Therefore, NERC concludes that any proposed definition of communication network "would need to be sufficiently broad to encompass all components in a communication network as they exist

[64] *Id.* P 150.

[65] *Id.* P 149 (referencing NIST SP 800-53 Revision 3, security control family Physical and Environmental Protection, Annex 2, page 54; BSI ISO/IEC (2005). *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2005).*British Standards Institute).

[66] NERC Petition at 52 (citing *North American Electric Reliability Corp.*, 142 FERC ¶ 61,203, at PP 13-14 (2013)).

now and in the future."[67] NERC explains that, based on that conclusion, the standard drafting team identified the types of equipment and components that responsible entities must protect, and developed reasonable controls to secure those components based on the risk they pose to the bulk electric system, rather than develop a specific definition.

48. NERC states that the revised CIP Reliability Standards, as proposed, address the ultimate security objective of protecting both the programmable and nonprogrammable components of communication networks.[68] NERC explains that the proposed standards include protections for cables and other nonprogrammable components of communication networks through proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10, which augments the existing protections for programmable communication components by requiring entities to implement various security controls to restrict and manage physical access to Physical Security Perimeters.[69] NERC further states that 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.[70]

---

[67] *Id.* at 52.

[68] *Id.*

[69] *Id.* at 52-53.

[70] *Id.* at 48.

49. NERC explains that proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 provides that, for High and Medium Impact BES Cyber Systems and their associated Protected Cyber Assets, responsible entities must restrict physical access to cabling and other nonprogrammable communication components used for connection between covered Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. NERC explains further that, where physical access restrictions to such cabling and components are not feasible, Part 1.10 provides that the responsible entity must document and implement encryption of data transmitted over such cabling and components and/or monitor the status of the communication link composed of such cabling and components. Further, pursuant to Part 1.10, a responsible entity must issue 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 implement an equally effective logical protection.[71]

50. NERC states that proposed Reliability Standard CIP-006-6 provides flexibility for responsible entities to implement the physical security measures that best suit their needs and to account for configurations where logical measures are necessary because the entity cannot implement physical access restrictions effectively. Responsible entities have the discretion as to the type of physical or logical protections to implement pursuant to

[71] *Id.* at 48-49.

Part 1.10, provided that the protections are designed to meet the overall security objective. According to NERC, 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 Protected Cyber Assets at control centers with High or Medium Impact BES Cyber Systems.[72]

51. NERC explains that proposed Part 1.10 applies only to nonprogrammable components outside of a Physical Security Perimeter because nonprogrammable components located within a Physical Security Perimeter are already subject to physical security protections by virtue of their location. NERC further states that Part 1.10 only applies to nonprogrammable components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter because Reliability Standard CIP-005-5 already requires logical protections for communications between discrete Electronic Security Perimeters.[73]

52. In addition, NERC asserts that the proposed Reliability Standards will strengthen the defense-in-depth approach by further minimizing the "attack surface" of BES Cyber Systems. NERC also clarifies that the standard drafting team limited the applicability in this manner to clarify that responsible entities are not responsible for protecting

[72] *Id.* at 49-50.

[73] *Id.* at 49.

nonprogrammable communication components outside of the responsible entity's control (i.e., components of a telecommunication carrier's network).[74]

Discussion

53. We believe that NERC's proposed alternative approach to addressing the Commission's Order No. 791 directive regarding the definition of communication networks adequately addresses part of the underlying concerns set forth in Order No. 791. Proposed Reliability Standard CIP-006-6, Requirement R1.10 specifies the types of assets subject to mandatory protection by using the existing definitions of Electronic Security Perimeter[75] and Physical Security Perimeter.[76] Proposed Reliability Standard CIP-006-6 addresses protection for non-programmable components of communication networks, such as network cabling and switches, that are located within the same Electronic Security Perimeter, but span separate Physical Security Perimeters. Specifically, proposed Reliability Standard CIP-006-6 requires responsible entities to restrict physical access to cabling and other nonprogrammable communication components between BES Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical

[74] *Id.* at 51.

[75] Electronic Security Perimeter: The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled. *See* NERC Glossary at 33.

[76] Physical Security Perimeter: The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled. *See* NERC Glossary at 60.

Security Perimeter. Where physical access restrictions to such cabling and components is not feasible, Part 1.10 provides that responsible entities must document and implement encryption of data transmitted over such cabling and components, monitor the status of the communication link composed of such cabling and components, or implement an equally effective logical protection.

54. We propose to accept NERC's proposed omission of a definition of communication networks based on NERC's explanation that responsible entities must develop controls to secure the non-programmable components of communication networks based on the risk they pose to the bulk electric system, rather than develop a specific definition of communication networks to identify assets for protection. NERC's proposal is an equally efficient and effective solution to the Commission's directive in Order No. 791 that NERC develop a definition of communication networks, subject to the proposed modification discussed below.

55. NERC's proposed solution for the protection of nonprogrammable components of communication networks, however, does not fully meet the intent of the Commission's Order No. 791 directive, resulting in a gap in security for bulk electric system communication systems. While the technical substance of CIP-006-6, Requirement R1, Part 1.10 appears to be adequate, we are concerned that the limited applicability of the provision results in limited protection for the nonprogrammable components of the communication systems at issue. Specifically, proposed CIP-006-6, Requirement R1, Part 1.10 would only apply to nonprogrammable components of communication networks within the same Electronic Security Perimeter, excluding from protection other

programmable and non-programmable communication network components that may exist outside of a discrete Electronic Security Perimeter.

56. While NERC asserts that this limitation is justified by the controls required under Reliability Standard CIP-005-5, NERC's position does not appear to consider that the controls set forth in Reliability Standard CIP-005-5 are limited to interactive remote access into an Electronic Security Perimeter, and can only be applied on programmable electronic devices and data that exists within an Electronic Security Perimeter.[77] This limitation would exclude communication network components that may be necessary to facilitate the automated transmission of reliability data between bulk electric system Control Centers in discrete Electronic Security Perimeters and would also exclude real time monitoring data that is used by Reliability Coordinators to monitor and assess the operation of their control areas. In other words, revised Reliability Standard CIP-006-6, Requirement R1 provides mandatory protection against: (1) physical attacks on nonprogrammable equipment; (2) man-in-the-middle attacks; and (3) session hijacking attacks within the confines of a bulk electric system Control Center, but does not extend protections to real-time data passing between Control Centers outside of a facility.

57. Comments from participants at the April 29, 2014 Technical Conference suggest that the Commission should take action to ensure the confidentiality, integrity, and availability of sensitive bulk electric system data when it is in motion both inside and

[77] *See* Reliability Standard CIP-005-5 (Electronic Security Perimeters), Requirement R2.

outside of an Electronic Security Perimeter.[78] We understand that inter-Control Center communications play a vital role in maintaining bulk electric system reliability and, as a result, we believe that the communication links and data used to control and monitor the bulk electric system should receive protection under the CIP Reliability Standards.

58. We also recognize that third party communication infrastructure (e.g., facilities owned by a telecommunications company) cannot necessarily be physically protected by responsible entities. This fact, however, does not alleviate the need to protect reliability data that traverses third party communication infrastructure. Proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 mandates that logical controls, such as encryption and connection link monitoring, be applied to cabling and components that cannot be physically restricted by the responsible entity. However, similar protections are not afforded to communications and data leaving bulk electric system Control Centers where they may be intercepted and altered while traversing communication networks.

59. Therefore, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop a modification to proposed Reliability Standard CIP-006-6 to require responsible entities to implement controls to protect, at a minimum, all communication links and sensitive bulk electric system data communicated between all bulk electric system Control Centers. This includes communication between two (or more) Control Centers, but not between a Control Center and non-Control Center facilities such as

[78] *See* Transcript at pp. 19, 24, 74-75 (Kevin Perry speaking), 79 (Mikhail Falkovich speaking).

substations. Also, if latency concerns mitigate against use of encryption as a logical control for any inter-Control Center communications, our understanding is that other logical protections are available, and we seek comment on this point.

60. Further, as discussed at the April 29, 2014 technical conference, panelists identified suggestions that could be explored to enhance protections for remote access, including the addition of logical or physical controls to provide additional network segmentation behind the intermediate systems. For example, the Commission is interested in comments that address the value achieved if the CIP standards were to require the incorporation of additional network segmentation controls, connection monitoring, and session termination controls behind responsible entity intermediate systems. We seek comment on whether these or other steps to improve remote access protection are needed, and whether the adoption of any additional security controls addressing this topic would provide substantial reliability and security benefits.

E. Risks Posed by Lack of Controls for Supply Chain Management

61. The information and communications technology and industrial control system supply chains provide hardware, software and operations support for computer networks. Such supply chains are complex, globally distributed and interconnected systems that have geographically diverse routes and consist of multiple tiers of outsourcing. The supply chain includes public and private sector entities that depend on each other to develop, integrate, and use information and communications technology and industrial control system supply chain products and services. Thus, the supply chain provides the

opportunity for significant benefits to customers, including low cost, interoperability, rapid innovation, a variety of product features and choice.

62. However, the global supply chain also enables opportunities for adversaries to directly or indirectly affect the management or operations of companies that may result in risks to the end user. Supply chain risks may include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices. To address these risks, NIST developed SP 800-161[79] to provide guidance and controls that can be used to comply with Federal Information Processing Standard 199 Standards for Security Categorization of Federal Information and Information Systems for Federal Government Information Systems.[80] Similarly, the Department of Energy has developed guidance on cybersecurity procurement language for energy delivery systems.[81]

63. While the Commission did not address supply chain management in Order No. 791, changes in the bulk electric system cyber threat landscape identified through recent malware campaigns targeting supply chain vendors have highlighted a gap in the

[79] NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015), *available at*: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[80] Federal Information Processing Standard Publication, *Standards for Security Categorization of Federal Information and Information Systems, available at*: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[81] *Cybersecurity Procurement Language for Energy Delivery Systems,* April 2014 at page 1. http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

protections under the CIP Standards. Specifically, in 2014, after Order No. 791 was issued, the Industry Control System - Computer Emergency Readiness Team (ICS-CERT) reported on two focused malware campaigns.[82] This new type of malware campaign is based on the injection of malware while a product or service remains in the control of the hardware or software vendor, prior to delivery to the customer.

64. We believe that it is reasonable to direct NERC to develop a new or modified Reliability Standard to provide security controls for supply chain management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The reliability goal should be to create a forward-looking, objective-driven standard that encompasses activities in the system development life cycle: from research and development, design and manufacturing stages (where applicable), to acquisition, delivery, integration, operations, retirement, and eventual disposal of the Registered Entity's information and communications technology and industrial control system supply chain equipment and services. The standard should support and ensure security, integrity, quality, and resilience of the supply chain and the future acquisition of products and services.

[82] ICS-CERT is a division of the Department of Homeland Security that works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community. *See* https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A; and https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B for "alert" information on supply chain malware campaigns.

65. Since security controls for supply chain management will likely vary greatly with each responsible entity due to variations in individual business practices, the right set of supply chain management security controls should accommodate for, among other things, an entity's: (1) procurement process; (2) vendor relations; (3) system requirements; (4) information technology implementation; and (5) privileged commercial or financial information. The following Supply Chain Risk Management controls from NIST SP 800-161 may be instructional in the development of any new reliability standard to address this security topic:[83] (1) Access Control Policy and Procedures; (2) Security Assessment Authorization; (3) Configuration Management; (4) Identification and Authentication; (5) System Maintenance Policy and Procedures; (6) Personnel Security Policy and Procedures; (7) System and Services Acquisition; (8) Supply Chain Protection; and (9) Component Authenticity.[84]

66. Therefore, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop a new reliability standard or modified reliability standard to provide security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. In addition to the parameters discussed above, due to the broadness of the topic and the individualized

[83] The listed controls do not reflect a comprehensive scope of the proposed standard.

[84] *See* NIST SP 800-161.

nature of many aspects of supply chain management, we anticipate that a Reliability Standard pertaining to supply chain management security would:

- Respect section 215 jurisdiction by only addressing the obligations of registered entities. A reliability standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities.
- Be forward-looking in the sense that the reliability standard should not dictate the abrogation or re-negotiation of currently-effective contracts with vendors, suppliers or other entities.
- Recognize the individualized nature of many aspects of supply chain management by setting goals (the "what"), while allowing flexibility in how a registered entity subject to the standard achieves that goal (the "how").[85]
- Given the types of specialty products involved and diversity of acquisition processes, the standard may need to allow exceptions, e.g., to meet safety requirements and fill operational gaps if no secure products are available.
- Provide enough specificity so that compliance obligations are clear and enforceable. In particular, we anticipate that a reliability standard that simply requires a registered entity to "have a plan" addressing supply chain management would not suffice. Rather, to adequately address our concerns, we

[85] *See* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 260.

> believe that a reliability standard should identify specific controls. As discussed above, NIST SP 800-161 may be instructional in identifying appropriate controls in the development of an effective supply chain management reliability standard.

We recognize that developing a supply chain management standard would likely be a significant undertaking and require extensive engagement with stakeholders to define the scope, content, and timing of the standard. Accordingly, to further that stakeholder engagement, we seek comment on this proposal, including: (1) the general proposal to direct that NERC develop a Reliability Standard to address supply chain management; (2) the anticipated features of, and requirements that should be included in, such a standard; and (3) a reasonable timeframe for development of a standard. We also direct staff, after receipt and consideration of those comments, to engage in additional outreach to further the Commission's consideration of the need for, and scope, content, and timing of, a supply chain management standard.

F. Proposed Definitions

67. The proposed revised CIP Reliability Standards include six new or revised definitions for inclusion in the NERC glossary. NERC's proposal includes four new definitions and two revised definitions. Specifically, NERC seeks approval for the following terms: (1) BES Cyber Asset; (2) Protected Cyber Asset; (3) Low Impact Electronic Access Point; (4) Low Impact External Routable Connectivity; (5) Removable Media; and (6) Transient Cyber Asset. We propose to approve the proposed definitions for inclusion in the NERC Glossary. We also seek comment on certain aspects of the

proposed definition for Low Impact External Routable Connectivity, as discussed below. After receiving comments, depending on the adequacy of the explanations provided in response to our questions, we may direct NERC to develop modifications to this definition to eliminate ambiguities and assure that the revised CIP Reliability Standards provide adequate protection for the bulk electric system.

Definition – Low Impact External Routable Connectivity

68. In its petition, NERC proposes the following definition for Low Impact External Routable Connectivity:

> 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 bidirectional 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).[86]

69. NERC explains that the proposed definition describes the scenarios where responsible entities are required to apply Low Impact access controls under Reliability Standard CIP-003-6, Requirement R2 to their Low Impact assets. Specifically, if Low Impact External Routable Connectivity is used, a responsible entity must implement a

[86] NERC Petition at 28.

Low Impact Electronic Access Point to permit only necessary inbound and outbound bidirectional routable protocol access.[87]

70. We seek comment on the following aspects of the proposed definition. First, we seek comment on the purpose of the meaning of the term "direct" in relation to the phrases "direct user-initiated interactive access" and "direct device-to-device connection" within the proposed definition. In addition, we seek comment on the implementation of the "layer 7 application layer break" contained in certain reference diagrams in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-003-6.[88] It appears that guidance provided in the Guidelines and Technical Basis section of the proposed standard may conflict with the plain reading of the term "direct." We are concerned that a conflict in the reading of the term "direct" could lead to complications in the implementation of the proposed CIP Reliability Standards, hindering the adoption of effective security controls for Low Impact BES Cyber Assets. Depending upon the responses received, we may direct NERC to develop a modification to the definition of Low Impact External Routable Connectivity.

G. Implementation Plan

71. NERC's proposed implementation plan for the proposed Reliability Standards is designed to match the effective dates of the proposed Reliability Standards with the

[87] *Id*. at 29.

[88] *See* CIP-003-6 Guidelines and Technical Basis Section, Reference Model 6 at p. 39.

effective dates of the prior versions of the related Reliability Standards under the implementation plan of the CIP version 5 Standards. NERC states that the purpose of this approach is to provide regulatory certainty by limiting the time, if any, that the CIP version 5 Standards with the "identify, assess, and correct" language would be effective. Specifically, pursuant to the CIP version 5 implementation plan, the effective date of each of the CIP version 5 Standards is April 1, 2016, except for the effective date for Requirement R2 of CIP-003-5, which 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 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 requirements applicable to Low Impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) until April 1, 2017.[89]

72. NERC's proposed implementation plan also includes effective dates for the new and modified definitions associated with: (1) transient devices (i.e., BES Cyber Asset, Protected Cyber Asset, Removable Media, and Transient Cyber Asset); and (2) Low Impact controls (i.e., Low Impact Electronic Access Point and Low Impact External Routable Connectivity). Specifically, NERC proposes: (1) that the definitions associated with transient device become effective on the compliance date for Reliability Standard

[89] *Id.* at 53-54.

CIP-010-2, Requirement R4; and (2) that the definitions addressing the Low Impact controls become enforceable on the compliance date for Reliability Standard CIP-003-6, Requirement R2. Lastly, NERC proposes 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 become effective on the effective date of the proposed Reliability Standards.[90]

73. We propose to approve NERC's implementation plan for the proposed CIP Reliability Standards, as described above.

H. Violation Risk Factor/Violation Severity Level Assignments

74. NERC requests approval of the violation risk factors and violation severity levels assigned to the proposed Reliability Standards. Specifically, NERC requests approval of 19 violation risk factor and violation severity level assignments associated with the proposed Reliability Standards.[91] We propose to accept these violation risk factors and violation severity levels.

III. Information Collection Statement

75. The FERC-725B information collection requirements contained in this Proposed Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[92] OMB's regulations require

[90] *Id.* at 56.

[91] *Id.*, Exhibit E.

[92] 44 U.S.C. 3507(d).

approval of certain information collection requirements imposed by agency rules.[93] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the Commission's need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

76. The Commission based its paperwork burden estimates on the changes in paperwork burden presented by the proposed CIP Reliability Standards as compared to the CIP version 5 Standards. The Commission has already addressed the burden of implementing the CIP version 5 Standards.[94] As discussed above, the immediate rulemaking addresses four areas of modification to the CIP standards: (1) removal of the "identify. assess, and correct" language from 17 CIP requirements; (2) development of enhanced security controls for low impact assets; (3) development of controls to protect transient devices (e.g. thumb drives and laptop computers); and (4) protection of communications networks. We do not anticipate that the removal of the "identify, assess

[93] 5 CFR 1320.11 (2012).

[94] *See* Order No. 791, 145 FERC ¶ 61,160 at PP 226-244.

and correct" language will impact the reporting burden, as the substantive compliance requirements would remain the same, while NERC indicates that the concept behind the deleted language continues to be implemented within NERC's compliance function. The development of controls to protect transient devices and protection of communication networks (as proposed by NERC) have associated reporting burdens that will affect a limited number of entities, i.e., those with Medium and High Impact BES Cyber Systems. The enhanced security controls for Low Impact assets are likely to impose a reporting burden on a much larger group of entities.

77. The NERC Compliance Registry, as of June 2015, identifies approximately 1,435 U.S. entities that are subject to mandatory compliance with Reliability Standards. Of this total, we estimate that 1,363 entities will face an increased paperwork burden under the proposed CIP Reliability Standards, and we estimate that a majority of these entities will have one or more Low Impact assets. In addition, we estimate that approximately 23 percent of the entities have assets that will be subject to Reliability Standards CIP-006-6 and CIP-010-2. Based on these assumptions, we estimate the following reporting burden:

Registered Entities	Number of Entities	Total Burden Hours in Year 1	Total Burden Hours in Year 2	Total Burden Hours in Year 3
Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets	313	75,120	130,208	130,208
Totals	313	75,120	130,208	130,208

78. The following shows the annual cost burden for each group, based on the burden hours in the table above:

- Year 1: Entities subject to CIP-006-6 and CIP-010-2 with Medium and/or High Impact Assets: 313 x 240 hours/entity * $76/hour = $5,709,120.
- Years 2 and 3: 313 entities x 416 hours/entity * $76/hour = $9,895,808 per year.
- The paperwork burden estimate includes costs associated with the initial development of a policy to address requirements relating to transient devices, as well as the ongoing data collection burden. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to policy development, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

Registered Entities	Number of Entities	Total Burden Hours in Year 1	Total Burden Hours in Year 2	Total Burden Hours in Year 3
Entities subject to CIP-003-6 with low impact Assets	1,363	163,560	283,504	283,504
Totals	1,363	163,560	283,504	283,504

79. The following shows the annual cost burden for each group, based on the burden hours in the table above:

- Year 1: Entities subject to CIP-003-6 with Low Impact Assets: 1,363 x 120 hours/entity * $76/hour = $12,430,560.
- Years 2 and 3: 1,363 entities x 208 hours/entity * $76/hour = $21,546,304 per year.
- The paperwork burden estimate includes costs associated with the modification of existing policies to address requirements relating to low impact assets, as well as the ongoing data collection burden, as set forth in CIP-003-6, Requirements R1.2 and R2, and Attachment 1. Further, the estimate reflects the assumption that costs incurred in year 1 will pertain to revising existing policies, while costs in years 2 and 3 will reflect the burden associated with maintaining logs and other records to demonstrate ongoing compliance.

80. The estimated hourly rate of $76 is the average loaded cost (wage plus benefits) of legal services ($129.68 per hour), technical employees ($58.17 per hour) and

administrative support ($39.12 per hour), based on hourly rates and average benefits data from the Bureau of Labor Statistics.[95]

81. Title: Mandatory Reliability Standards, Revised Critical Infrastructure Protection Standards.

Action: Proposed Collection FERC-725B.

OMB Control No.: 1902-0248.

Respondents: Businesses or other for-profit institutions; not-for-profit institutions.

Frequency of Responses: On Occasion.

Necessity of the Information: This proposed rule proposes to approve the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission proposes to approve NERC's proposed revised CIP Reliability Standards pursuant to section 215(d)(2) of the FPA because they improve the currently-effective suite of cyber security CIP Reliability Standards.

Internal Review: The Commission has reviewed the proposed Reliability Standards and made a determination that its action is necessary to implement section 215 of the FPA.

82. Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].

---

[95] *See* http://bls.gov/oes/current/naics2_22.htm and http://www.bls.gov/news.release/ecec.nr0.htm. Hourly figures as of June 1, 2015.

83. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM15-14-000 and OMB Control Number 1902-0248.

IV. Regulatory Flexibility Act Analysis

84. The Regulatory Flexibility Act of 1980 (RFA) generally requires a description and analysis of Proposed Rules that will have significant economic impact on a substantial number of small entities.[96] The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[97] The SBA revised its size standard for electric utilities (effective January 22, 2014) to a standard based on the number of employees, including affiliates (from the prior standard based on megawatt hour sales).[98] Proposed Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 are expected to impose an additional

[96] 5 U.S.C. 601-12.

[97] 13 C.F.R. 121.101 (2013).

[98] SBA Final Rule on "Small Business Size Standards: Utilities," 78 FR 77343 (Dec. 23, 2013).

burden on 1,363 entities[99] (reliability coordinators, generator operators, generator owners, interchange coordinators or authorities, transmission operators, balancing authorities, transmission owners, and certain distribution providers).

85. Of the 1,363 affected entities discussed above, we estimate that 444 entities are small entities. We estimate that 399 of these 444 small entities do not own BES Cyber Assets or BES Cyber Systems that are classified as Medium or High Impact and, therefore, will only be affected by the proposed modifications to Reliability Standard CIP-003-6. As discussed above, proposed Reliability Standard CIP-003-6 enhances reliability by providing criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact BES Cyber Assets. We estimate that each of the 399 small entities to whom the proposed modifications to Reliability Standard CIP-003-6 applies will incur one-time costs of approximately $149,358 per entity to implement this standard, as well as the ongoing paperwork burden reflected in the Information Collection Statement (approximately $15,000 per year per entity). We do not consider the estimated costs for these 399 small entities a significant economic impact.

86. In addition, we estimate that 14 small entities own Medium Impact substations and that 31 small transmission operators own Medium or High impact control centers. These

[99] Public utilities may fall under one of several different categories, each with a size threshold based on the company's number of employees, including affiliates, the parent company, and subsidiaries. For the analysis in this NOPR, we are using a 500 employee threshold for each affected entity to conduct a comprehensive analysis.

45 small entities represent 10.1 percent of the 444 affected small entities. We estimate that each of these 45 small entities may experience an economic impact of $50,000 per entity in the first year of initial implementation to meet proposed Reliability Standard CIP-010-2 and $30,000 in ongoing annual costs,[100] for a total of $110,000 per entity over the first three years. Therefore, we estimate that each of these 45 small entities will incur a total of $258,654 in costs over the first three years. We conclude that 10.1 percent of the total 444 affected small entities does not represent a substantial number in terms of the total number of regulated small entities.

87. Based on the above analysis, we propose to certify that the proposed Reliability Standards will not have a significant economic impact on a substantial number of small entities.

V. Environmental Analysis

88. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect on the human environment.[101] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being

[100] Estimated annual cost for year 2 and forward.

[101] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987).

amended.[102] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

VI. Comment Procedures

89. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due [**INSERT DATE 60 days after publication in the FEDERAL REGISTER**]. Comments must refer to Docket No. RM15-14-000, and must include the commenter's name, the organization they represent, if applicable, and address.

90. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

91. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

92. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability

[102] 18 C.F.R. 380.4(a)(2)(ii).

section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VII. Document Availability

93. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

94. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number of this document, excluding the last three digits, in the docket number field.

User assistance is available for eLibrary and the Commission’s website during normal business hours from the Commission’s Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or e-mail at ferconlinesupport@ferc.gov, or the Public Reference

Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.