145 FERC ¶ 61,160
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

Docket No. RM13-5-000

Version 5 Critical Infrastructure Protection Reliability Standards

(Issued November 22, 2013)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

SUMMARY: Pursuant to section 215 of the Federal Power Act, the Commission approves the Version 5 Critical Infrastructure Protection Reliability Standards, CIP-002-5 through CIP-011-1, submitted by the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization. The CIP version 5 Standards address the cyber security of the bulk electric system and are an improvement over the current Commission-approved CIP Reliability Standards. The CIP version 5 Standards adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards. The Commission also approves nineteen new or revised definitions associated with the CIP version 5 Standards for inclusion in the Glossary of Terms Used in NERC Reliability Standards. In addition, the Commission directs NERC to develop modifications to the CIP version 5 Standards and submit informational filings.

EFFECTIVE DATE: This rule will become effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT:

Austin Rappeport (Technical Information)
Office of Electric Reliability, Division of Reliability Standards and Security
Federal Energy Regulatory Commission
1800 Dual Highway, Suite 201
Hagerstown, MD 21740
Telephone: (301) 665-1393

Daniel Phillips (Technical Information)
Office of Electric Reliability, Division of Reliability Standards and Security
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-6387

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-6840

Matthew Vlissides (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
Telephone: (202) 502-8408

SUPPLEMENTARY INFORMATION:

145 FERC ¶ 61,160
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Philip D. Moeller, John R. Norris,
Cheryl A. LaFleur, and Tony Clark.

Version 5 Critical Infrastructure Protection Reliability Standards — Docket No. RM13-5-000

ORDER NO. 791

FINAL RULE

(Issued November 22, 2013)

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission approves the Version 5 Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-5 through CIP-011-1, submitted by the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO). The CIP version 5 Standards address the cyber security of the bulk electric system and are an improvement over the current Commission-approved CIP Reliability Standards. The CIP version 5 Standards adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards. The Commission also approves nineteen new or revised definitions associated with the CIP version 5 Standards for inclusion in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

[1] 16 U.S.C. 824o (2012).

2. The CIP version 5 Standards 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. At a minimum, a BES Cyber System must be categorized as a Low Impact asset. Once a BES Cyber System is categorized, a responsible entity must comply with the associated requirements of the CIP version 5 Standards that apply to the impact category. The CIP version 5 Standards also include 12 requirements with new cyber security controls, which address Electronic Security Perimeters (CIP-005-5), Systems Security Management (CIP-007-5), Incident Reporting and Response Planning (CIP-008-5), Recovery Plans for BES Cyber Systems (CIP-009-5), and Configuration Change Management and Vulnerability Assessments (CIP-010-1).

The CIP version 5 Standards are an improvement over the currently-approved CIP Reliability Standards. The Commission determines that categorizing BES Cyber Systems based on their Low, Medium, or High Impact on the reliable operation of the bulk electric system, with all BES Cyber Systems being categorized as at least Low Impact, offers more comprehensive protection of the bulk electric system. The Commission also finds that the new cyber security controls improve the security posture of responsible entities. Accordingly, the Commission approves the CIP version 5 Standards.

3. In addition to approving the CIP version 5 Standards, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop modifications to the CIP version 5 Standards. As discussed below, we also direct NERC to submit informational filings

regarding certain issues during and following implementation of the CIP version 5 Standards.[2]

4. First, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to remove language found in 17 requirements in the CIP version 5 Standards that requires responsible entities to implement the requirements in a manner to "identify, assess, and correct" deficiencies.[3] We support NERC's move away from a "zero tolerance" approach to compliance, the development of strong internal controls by responsible entities, and NERC's development of standards that focus on the activities that have the greatest impact on Bulk-Power System reliability. However, the Commission is concerned that the proposed language is overly-vague, lacking basic definition and guidance that is needed, for example, to distinguish a successful internal control program from one that is inadequate. Alternatively, NERC may propose modifications that address the Commission concerns, discussed below, regarding the ambiguity and enforceability of the "identify, assess, and correct" language. The Commission directs NERC to submit a proposal for Commission approval within one year from the effective date of this Final Rule.[4]

---

[2] We note that the informational filings directed in this Final Rule are for informational purposes only and will not be noticed, nor require Commission action.

[3] *See* NERC Petition at 33.

[4] The proposed one year deadline would pertain only to addressing the "identify, assess and correct" language and the directive concerning communication networks, not to the other proposed modifications discussed below.

5. Second, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop modifications that address security controls for Low Impact assets. As discussed below, the adoption of the Low Impact BES Cyber Asset category will expand the protections offered by the CIP version 5 Standards to additional assets that could cause cyber security risks to the bulk electric system. Specifically, categorizing BES Cyber Systems based on their Low, Medium, or High Impact on the reliable operation of the bulk electric system, with all BES Cyber Systems being categorized as at least Low Impact, offers more comprehensive protection of the bulk electric system. However, the CIP version 5 Standards do not require specific controls for Low Impact assets nor do they contain objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities for Low Impact assets. As discussed below, we direct that NERC develop modifications to the CIP version 5 Standards to address this concern. While NERC may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.

6. Third, we approve the definition of BES Cyber Asset. In addition, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop requirements that protect transient electronic devices (*e.g.*, thumb drives and laptop computers) that fall outside of the BES Cyber Asset definition.[5] While we are persuaded by NERC and others that it

[5] As discussed below, NERC's definition of BES Cyber Asset provides that a "Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is

(continued…)

would be burdensome to include transient devices as BES Cyber Assets, we also believe that further protections are needed in light of the potential vulnerabilities associated with transient devices. Further, as discussed below, to better understand the scope and reach of the term BES Cyber Asset, we direct NERC to conduct a survey of responsible entities during the CIP version 5 Standards implementation periods to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter.[6] The Commission directs NERC to submit an informational filing one year from the effective date of this Final Rule that assesses, based on the survey results, whether the BES Cyber Asset definition will, with the 15-minute parameter, cover the assets that are necessary to ensure the reliable operation of the Bulk-Power System.

7. Fourth, the Commission approves the definition of Cyber Asset. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to create a definition of communication networks and to develop new or modified Reliability Standards that address the protection of communication networks. The Commission also

---

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."

[6] NERC's BES Cyber Asset definition only includes Cyber Assets that "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment…."

directs its staff to include the issue of protecting the nonprogrammable components of communications networks in the staff-led technical conference discussed herein.

8. The Commission approves 30 of the 32 Violation Risk Factors (VRF) proposed by NERC. However, the Commission directs NERC to modify the VRF assignment for Reliability Standard CIP-006-5, Requirement R3 from Lower to Medium and to modify the VRF assigned to Reliability Standard CIP-004-5, Requirement R4 from Lower to Medium. In addition, we direct NERC to modify eight of the Violation Severity Levels (VSLs) for the CIP version 5 Standards.

9. The Commission approves NERC's proposal to allow responsible entities to transition from compliance with the currently-effective CIP version 3 Standards to compliance with the CIP version 5 Standards. Thus, CIP-002-4 through CIP-009-4 will not become effective, and CIP-002-3 through CIP-009-3 will remain in effect until the effective date of the CIP version 5 Standards.[7] The Commission also approves the implementation plan and effective dates proposed by NERC.

I. Background

A. Section 215 of the FPA

10. Section 215 of the FPA requires the Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and

[7] On August 12, 2013, the Commission granted an extension of time to implement the CIP version 4 Standards from April 1, 2014 to October 1, 2014. *N. Am. Elec. Reliability Corp.*, 144 FERC ¶ 61,123 (2013).

approval. Once approved, the Reliability Standards may be enforced in the United States by the ERO, subject to Commission oversight, or by the Commission independently.[8] Pursuant to the requirements of FPA section 215, the Commission established a process to select and certify an ERO.[9] The Commission subsequently certified NERC as the ERO.[10]

B. Order Nos. 706 and 761

1. Order No. 706

11. On January 18, 2008, the Commission issued Order No. 706, which approved the CIP version 1 Standards to address cyber security of the Bulk-Power System.[11] In Order No. 706, the Commission approved eight CIP Reliability Standards (CIP-002-1 through CIP-009-1). While approving the CIP version 1 Standards, the Commission also directed NERC to develop modifications to them to enhance the protection provided by the CIP Reliability Standards. Subsequently, NERC filed the CIP version 2 and CIP version 3

[8] 16 U.S.C. 824o(e)(3) (2012).

[9] *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).

[10] *N. Am. Elec. 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).

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

Standards in partial compliance with Order No. 706. The Commission approved these Reliability Standards in September 2009[12] and March 2010,[13] respectively.

2. Order No. 761

12. On April 19, 2012, the Commission issued Order No. 761, which approved the CIP version 4 Standards (CIP-002-4 through CIP-009-4).[14] Reliability Standard CIP-002-4 (Critical Cyber Asset Identification) sets forth 17 uniform "bright line" criteria for identifying Critical Assets. The Commission also accepted NERC's proposed implementation schedule for the CIP version 4 Standards, which are currently scheduled to be fully implemented and enforceable beginning October 2014.[15]

C. NERC Petition and CIP Version 5 Standards

1. NERC Petition and Errata

13. In its January 31, 2013 petition, NERC seeks Commission approval of the CIP version 5 Standards, nineteen new or revised NERC Glossary terms, VRF and VSL

[12] *N. Am. Elec. Reliability Corp.*, 128 FERC ¶ 61,291, *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009).

[13] *N. Am. Elec. Reliability Corp.*, 130 FERC ¶ 61,271 (2010).

[14] *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 Fed. Reg. 24,594 (Apr. 25, 2012), 139 FERC ¶ 61,058 (2012), *order denying reh'g*, 140 FERC ¶ 61,109 (2012).

[15] As noted above, the Commission extended the compliance deadline for the CIP version 4 Standards in Order No. 761 from April 2014 to October 2014.

assignments, and an implementation plan.[16] NERC maintains that the CIP version 5 Standards are just and reasonable, as they meet or exceed each of the guidelines that the Commission identified in Order No. 672 for evaluating a proposed Reliability Standard.[17] NERC asserts that the CIP version 5 Standards "serve the important reliability goal of providing a cybersecurity framework for the identification and protection of BES Cyber Systems … to support the reliable operation of the Bulk Power System."[18] In addition, NERC states that the CIP version 5 Standards are "designed to be clear and unambiguous" and the Commission should approve the CIP version 5 Standards as "clearly enforceable."[19]

14. Further, NERC maintains that the CIP version 5 Standards represent a significant improvement to the currently-approved CIP Reliability Standards, as the CIP version 5 Standards require responsible entities to use a new approach to categorize all cyber systems impacting the bulk electric system as having a Low, Medium, or High Impact.[20]

---

[16] Reliability Standards CIP-002-5 through CIP-011-1 are not attached to this Final Rule. The complete text of CIP version 5 Standards is available on the Commission's eLibrary document retrieval system in Docket No. RM13-5-000 and is posted on the ERO's web site, *available at* http://www.nerc.com.

[17] *See* NERC Petition at 8 (citing Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 320-337). *See also* NERC Petition, Exh. G (Order No. 672 Criteria for Approving Proposed Reliability Standards).

[18] *Id.* at 10.

[19] *Id.* at 27.

[20] *See id.* at 15.

NERC states that the new approach to classifying cyber systems "moves away from the CIP version 4 'bright-line' approach of only identifying Critical Assets (and applying CIP requirements only to their associated Critical Cyber Assets), to requiring a minimum classification of 'Low Impact' for all BES Cyber Systems."[21] NERC states that the adoption of the Low-Medium-High Impact categorization "resulted from a review of the National Institute of Standards and Technology (NIST) Risk Management Framework for categorizing and applying security controls, a review that was directed by the Commission in Order No. 706."[22]

15. NERC also notes the adoption of new language within several of the CIP version 5 Standards in which the standard drafting team incorporated "a requirement that Responsible Entities implement cyber policies in a manner to 'identify, assess, and correct' deficiencies."[23] NERC states that the "identify, assess, and correct" language is "[c]onsistent with the NIST Risk Management Framework and the Commission's guidance in prior orders," asserting that the "implementation of certain CIP version 5 requirements in a manner to 'identify, assess, and correct' deficiencies emulates the *FERC Policy Statement on Penalty Guidelines*."[24] NERC further states that the "identify,

[21] *Id.*

[22] *Id.*

[23] *Id.* at 33.

[24] *Id.*

assess, and correct" language "is included as a performance expectation in the requirements, not as an enforcement component."[25]

16. NERC asserts that the CIP version 5 Standards address "all applicable directives in Order No. 706" while "eliminating unnecessary documentation requirements to allow entities to focus on the reliability and security of the Bulk Power System."[26] Accordingly, NERC requests that the Commission approve the CIP version 5 Standards, the new and revised definitions, the associated VRF and VSL assignments, and the implementation plan. NERC requests that the CIP version 5 Standards become effective on "the first day of the eighth calendar quarter after a Final Rule is issued in this docket."[27]

17. NERC requests prompt Commission action approving the CIP version 5 Standards and associated implementation plan.[28] With regard to the implementation plan, NERC states that the proposed language "would allow entities to transition from CIP Version 3 to CIP Version 5, thereby bypassing implementation of CIP Version 4 completely upon Commission approval."[29] NERC asserts that prompt approval of the CIP version 5

---

[25] *Id.*

[26] *Id.* at 5.

[27] *Id.* at 2.

[28] *Id.* at 5.

[29] *Id.* at 4.

Standards and implementation plan "would reduce uncertainty among Responsible Entities regarding implementation of the CIP standards."[30]

18. On September 30, 2013, NERC filed an errata with corrections to the VSLs for the CIP version 5 Standards and revisions to the definitions of Electronic Access Control or Monitoring Systems and Interactive Remote Access in which the term "Intermediate Devices" is replaced with the term "Intermediate Systems." On October 1, 2013, NERC filed a supplemental errata to correct a formatting error in the September 30 errata.

2. CIP Version 5 Standards and NERC Explanation of Provisions

19. The CIP version 5 Standards include ten new or modified Reliability Standards.

20. **CIP-002-5 – Cyber Security – BES Cyber System Categorization**: CIP-002-5 is the first step in identifying BES Cyber Systems, which are assets which must be protected by the cyber security standards. If a responsible entity does not identify any BES Cyber Systems, it does not have compliance responsibility under the rest of the proposed CIP Standards. However, a responsible entity that identifies BES Cyber Systems must comply with CIP-003-5 to CIP-011-1, according to specific criteria that characterize the impact of the identified BES Cyber Systems.

21. In particular, CIP-002-5 adds two new terms to the NERC Glossary that define the assets subject to CIP protections. First, NERC defines a BES Cyber Asset as "[a] Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its

[30] *Id.* at 5.

required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System."[31] Second, NERC defines a BES Cyber System as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."[32]

22. NERC states that Reliability Standard CIP-002-5 will require the identification and categorization of BES Cyber Systems according to specific criteria that characterize their impact for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the bulk electric system.[33]

23. NERC states that CIP-002-5 "Attachment 1 – Impact Rating Criteria" identifies three categories of BES Cyber Systems. The High Impact category covers large control centers, similar to those control centers identified as Critical Assets in CIP-002-4. The Medium Impact category covers generation and transmission facilities, similar to those identified as Critical Assets in CIP-002-4, along with other control centers not identified as Critical Assets in CIP-002-4. The Low Impact category covers all other BES Cyber

[31] *Id.* at 14.

[32] *Id.*

[33] *Id.* at 11.

Systems. NERC states that the Low Impact category provides protections for systems not included in the CIP version 4 Standards.[34]

24. Once a responsible entity identifies a BES Cyber System under CIP-002-5, the entity must comply with the controls included in Reliability Standards CIP-003-5 to CIP-011-1 corresponding to its impact category.[35]

25. **CIP-003-5 – Cyber Security – Security Management Controls:** NERC states that Reliability Standard CIP-003-5 will require approval by a CIP Senior Manager of the documented cyber security policies related to CIP-004-5 through CIP-009-5, CIP-010-1, and CIP-011-1. Reliability Standard CIP-003-5, Requirement R2, will require implementation of policies related to cyber security awareness, physical security controls, electronic access controls, and incident response to a Cyber Security Incident for those assets that have Low Impact BES Cyber Systems under CIP-002-5's categorization process. According to NERC, a requirement that a Cyber Security Policy be "readily available" was deleted because of general confusion around that term and because training requirements in CIP-004-5 provide for knowledge of reliability policies. NERC states that it moved several provisions of requirements related to information

[34] *Id.*

[35] *Id.*

protection in previous CIP versions to CIP-011-1 and, therefore, deleted the requirements from CIP-003-5.[36]

26. **CIP-004-5 – Cyber Security – Personnel and Training:** NERC states that Reliability Standard CIP-004-5 will require documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management. Requirement R2 of CIP-004-5 adds specific training roles for visitor control programs, electronic interconnectivity supporting the operation and control of BES Cyber Systems, and storage media as part of the treatment of BES Cyber System Information. NERC states that the drafting team modified the requirements pertaining to personnel risk assessments and access management in response to lessons learned from implementing previous versions. Reliability Standard CIP-004-5, Requirement R3, now specifies that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more without specifying school, work, etc., and regardless of official residence. Reliability Standard CIP-004-5, Requirement R4 now combines the access management requirements from CIP-003-4, CIP-004-4, CIP-006-4, and CIP-007-4 into a single requirement. These requirements from the CIP version 4 Standards, as incorporated in Requirement R4, remain largely unchanged except to clarify certain terminology. NERC states that combining these requirements improves consistency in the authorization and review process. Reliability

[36] *Id.* at 11-12.

Standard CIP-004-5 modifies Requirement R4 by removing the obligation to maintain a list of authorized personnel. NERC explains that the removal is appropriate because the list represents only one form of evidence to demonstrate compliance that only authorized persons have access. Requirement R5 requires a registered entity to revoke a terminated employee's access concurrent with his or her termination, to be completed within 24 hours.[37]

27. **CIP-005-5 – Cyber Security – Electronic Security Perimeter(s):** NERC states that Reliability Standard CIP-005-5, Requirement R1, focuses on the discrete Electronic Access Points rather than the logical "perimeter," which is the focus of currently-effective CIP-005-3. Requirement R1.2 of the currently-effective CIP-005-3 has been deleted from the CIP version 5 Standards. NERC explains that Requirement R1.2 is definitional and was used to bring dial-up modems using non-routable protocols into the scope of previous versions of CIP-005. According to NERC, the non-routable blanket exemption included in the CIP version 1 through version 4 Standards was removed from CIP-002-5.

28. **CIP-006-5 – Cyber Security – Physical Security of BES Cyber Systems**: NERC states that Reliability Standard CIP-006-5 is intended to manage physical access to BES Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability. Reliability

[37] *Id.* at 12.

Standard CIP-006-5 reflects the retirement of Requirements R8.2 and R8.3 of Commission-approved CIP-006-4, concerning the retention of testing records. According to NERC, the retention period is now specified in the compliance section of Reliability Standard CIP-006-5.[38]

29. **CIP-007-5 – Cyber Security – Systems Security Management:** NERC states that Reliability Standard CIP-007-5 addresses system security by specifying technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability of the bulk electric system. NERC states that it modified CIP-007-5 to conform to the formatting approach of the CIP version 5 Standards, along with changes to address several Commission directives and to make the requirements less dependent on specific technology so that they will remain relevant for future, yet-unknown developing technologies. For example, according to NERC, Requirement R3 is a competency-based requirement, i.e., the responsible entity must document how it addresses the malware risk for each BES Cyber System, but the requirement does not prescribe a particular technical method in order to account for potential technological advancement.[39]

30. **CIP-008-5 – Cyber Security – Incident Reporting and Response Planning:** NERC states that Reliability Standard CIP-008-5 mitigates the risk to the reliable

[38] *Id.*

[39] *Id.* at 12-13.

operation of the bulk electric system resulting from a Cyber Security Incident by specifying incident response requirements. Proposed Requirement R1 requires responsible entities to report Cyber Security Incidents within 1 hour of recognition. Requirement R2 requires testing to verify response plan effectiveness and consistent application in responding to a Cyber Security Incident. Requirement R3 provides for an after-action review for tests or actual incidents, and requires an update to the Cyber Security Incident response plan based on those lessons learned. Requirement R3 also establishes a single timeline for a responsible entity to determine the lessons learned and update recovery plans. Specifically, where previous CIP versions specified "30 calendar days" for determining the lessons learned, followed by additional time for updating recovery plans and notification, proposed Requirement R3 combines those activities into a single 90-day timeframe.[40]

31. **CIP-009-5 – Cyber Security – Recovery Plans for BES Cyber Systems:** NERC explains that Reliability Standard CIP-009-5 provides for the recovery of the reliability functions performed by BES Cyber Systems by specifying a recovery plan to support the continued stability, operability, and reliability of the bulk electric system. Requirement R1 includes controls to protect data that would be useful in the investigation of an event that results in the execution of a Cyber System recovery plan. NERC explains that Requirement R2 includes operational testing to support the recovery of BES Cyber

[40] *Id.* at 13.

Systems. Requirement R3 establishes a single timeline for a responsible entity to determine the lessons learned and update recovery plans, similar to CIP-008-5.[41]

32. **CIP-010-1 – Cyber Security – Configuration Change Management and Vulnerability Assessments:** NERC states that Reliability Standard CIP-010-1 is a new Reliability Standard consolidating the configuration change management and vulnerability assessment-related requirements from previous versions of CIP-003, CIP-005 and CIP-007. Requirement R1 specifies the configuration change management requirements. Requirement R2 establishes the configuration monitoring requirements intended to detect unauthorized modifications to BES Cyber Systems. NERC explains that Requirement R3 establishes the vulnerability assessment requirements intended to ensure proper implementation of cyber security controls while promoting continuous improvement of a responsible entity's cyber security posture.[42]

33. **CIP-011-1 – Cyber Security – Information Protection:** NERC states that Reliability Standard CIP-011-1 is a new Reliability Standard consolidating the information protection requirements from previous versions of CIP-003 and CIP-007. Requirement R1 specifies information protection controls to prevent unauthorized access

[41] *Id.*

[42] *Id.*

to BES Cyber System Information. Requirement R2 specifies reuse and disposal provisions to prevent unauthorized dissemination of protected information.[43]

D. Notice of Proposed Rulemaking

34. On April 18, 2013, the Commission issued a Notice of Proposed Rulemaking proposing to approve the CIP version 5 Standards, CIP-002-5 through CIP-011-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.[44] The NOPR stated that the CIP version 5 Standards adopt new cyber security controls that are intended to safeguard physical and electronic access to BES Cyber Systems. Further, the NOPR stated that NERC proposes a new approach to identifying and classifying BES Cyber Systems that will require at least a minimum classification of Low Impact for all BES Cyber Systems. The NOPR also proposed to approve the nineteen new or revised definitions associated with the CIP version 5 Standards for inclusion in the NERC Glossary.

35. While proposing to approve the CIP version 5 Standards, the Commission also identified issues with the CIP version 5 Standards. The Commission stated in the NOPR that NERC's proposal to include language that requires entities to "identify, assess, and correct" deficiencies is unclear with respect to the implementation and compliance obligations that language imposes and that it is too vague to audit and enforce

[43] *Id.* at 13-14.

[44] *Version 5 Critical Infrastructure Protection Reliability Standards*, 78 FR 24,107 (Apr. 24, 2013), 143 FERC ¶ 61,055 (2013) (NOPRA).

compliance. The NOPR sought comment on the "identify, assess, and correct" language and stated that, depending on the comments, the Commission may direct NERC to develop modifications or remove the "identify, assess, and correct" language. In addition, the NOPR proposed to direct NERC to modify Reliability Standard CIP-003-5, Requirement R2, to require responsible entities to adopt specific, technically-supported cyber security controls for Low Impact BES Cyber Assets. The NOPR sought comment on these proposals.

36. The NOPR identified issues with the proposed definitions of BES Cyber Asset, Control Center, and Cyber Asset and use of the terms Reliability Tasks and Intermediate Devices in the proposed definitions. In addition, the NOPR identified technical issues involving improvements to the CIP version 5 Standards, including remote access, communications security, and the NIST Risk Management Framework. The NOPR stated that, depending on the comments received, the Commission may direct NERC to develop modifications to certain definitions to eliminate ambiguities and ensure that BES Cyber Assets are adequately protected. The NOPR sought comment on these proposals.

37. In the NOPR, the Commission proposed to approve 30 of the 32 VRFs. In addition, the Commission proposed to direct NERC to modify the VSLs for the CIP version 5 Standards.

38. The Commission proposed in the NOPR to approve NERC's proposal to allow responsible entities to transition from compliance with the currently-effective CIP version 3 Standards to compliance with the CIP version 5 Standards, essentially retiring the CIP version 4 Standards prior to mandatory compliance. The NOPR also sought comment on

whether the 24-month and 36-month implementation periods proposed by NERC for the CIP version 5 Standards are necessary, and what activities are required to effect the transition during the proposed implementation periods.

39. In response to the NOPR, interested entities filed 62 comments. The comments have assisted us in better understanding the issues and developing this Final Rule. We address below the issues raised in the NOPR and comments. The Appendix to this Final Rule lists the entities that filed comments on the NOPR.

E. NERC Informational Filing

40. On October 11, 2013, NERC submitted an informational filing detailing a pilot program to be conducted during the transition from the CIP version 3 Standards to the CIP version 5 Standards. NERC explains that the implementation study is part of a larger program that includes the development of guidance, outreach to industry, and training for all responsible entities throughout the implementation period.[45] NERC states that the goals of the implementation study include: (1) improving industry's understanding of the technical security challenges that need to be addressed in order to comply with the CIP version 5 Standards; (2) providing industry with a clear approach to transition from the CIP version 3 Standards to the CIP version 5 Standards, including compliance and enforcement expectations; and (3) providing industry with the knowledge to understand the technical and compliance-related resources needed to transition to, and manage

[45] NERC Informational Filing at 7.

compliance with, the CIP version 5 Standards.[46] NERC explains further that the study participants will consist of seven representative responsible entities with a proven record of success in compliance with the CIP version 3 Standards.[47] NERC states that based on participation in the implementation study, future compliance with the CIP version 3 Standards will be waived for these seven responsible entities.[48] Finally, NERC concludes that following the conclusion of the implementation study in April 2014, NERC and the Regional Entities will prepare and publish a report that identifies the lessons learned and recommendations for the transition to the CIP version 5 Standards resulting from the implementation study.[49]

II. Discussion

41. Pursuant to section 215(d) of the FPA, the Commission approves the CIP version 5 Standards, CIP-002-5 through CIP-011-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We find that the CIP version 5 Standards represent an improvement over the currently-approved CIP Reliability Standards. In particular, we find that the categorization of assets under CIP-002-5 based on their Low, Medium, or High Impact on the reliable operation of the bulk electric system, with all

[46] *Id.* at 7-8.

[47] *Id.* at 8.

[48] *Id.* at 12-13.

[49] *Id.* at 3.

BES Cyber Systems being categorized as at least Low Impact, offers more comprehensive protection of the bulk electric system. In addition, the CIP version 5 Standards incorporate several new cyber security controls that will improve the overall security posture of the responsible entities. Further, we approve nineteen new or revised definitions associated with the CIP version 5 Standards for inclusion in the NERC Glossary. We approve the implementation plan and, with modifications, VRFs and VSLs proposed by NERC.

42. As discussed below, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop modifications to the CIP version 5 Standards to address our concerns regarding: (1) the "identify, assess, and correct" language; (2) protections for Low Impact BES Cyber Systems; (3) the risks posed by transient devices; and (4) the protection of communication networks. Further, we direct that NERC survey responsible entities during the CIP version 5 Standards implementation periods to gain a better understanding of the BES Cyber Asset definition. In addition, the Commission directs staff to convene a staff-led technical conference, within 180 days from the date of this Final Rule, addressing the technical issues identified in the NOPR concerning communications security, remote access, and the NIST Risk Management Framework.

43. Below we discuss the following matters: (A) the "identify, assess, and correct" language; (B) BES Cyber Asset categorization; (C) new and revised NERC Glossary definitions; (D) implementation plan; (E) VRF and VSL assignments; and (F) other technical issues.

A. "Identify, Assess, and Correct" Language

NERC Petition

44. The CIP version 5 Standards incorporate "a requirement that Responsible Entities implement cyber policies in a manner to 'identify, assess, and correct' deficiencies" in 17 CIP requirements.[50] NERC states that the "identify, assess, and correct" language is "[c]onsistent with the NIST Risk Management Framework and the Commission's guidance in prior orders," asserting that the "implementation of certain CIP version 5 requirements in a manner to 'identify, assess, and correct' deficiencies emulates the *FERC Policy Statement on Penalty Guidelines*."[51]

NOPR

45. In the NOPR, the Commission stated that NERC has not explained the proposed "identify, assess, and correct" language sufficiently. The NOPR expressed concern that this language is unclear as to the implementation and compliance obligations it places on responsible entities and is too vague to audit and enforce compliance. The NOPR sought comment on the meaning of this language and on how it will be implemented and enforced. The NOPR stated that, depending on the explanations provided in the comments, the Commission may direct NERC to develop modifications, including directing NERC to clarify both the implementation and compliance obligations created

[50] NERC Petition at 33.

[51] *Id.*

by this language and the criteria by which auditors will be able to determine compliance, or the Commission may direct NERC to remove this language if it results in requirements that degrade the protections afforded by the CIP version 5 Standards and are difficult to implement and enforce.

46. The NOPR questioned whether the "identify, assess, and correct" language imposes one obligation on a responsible entity (i.e., to ensure the entity has a process in place to "identify, assess, and correct" a violation or, alternatively, to ensure that the underlying substantive requirement is not violated) or two obligations (i.e., to (1) ensure the entity has a process in place to "identify, assess, and correct" a violation and (2) to ensure that the underlying substantive requirement is not violated). The NOPR stated that the proposed "identify, assess, and correct" language is ambiguous enough to support both interpretations. The NOPR expressed concern that, under either interpretation, the "identify, assess, and correct" language is too vague to be audited, and that NERC has not explained what is expected of responsible entities or the intended meaning of the individual terms "identify," "assess," "correct," and "deficiencies" as they are used in the CIP version 5 Standards.

47. With respect to the term "identify," the NOPR observed that it is not clear whether a responsible entity is expected to take steps to recognize past deficiencies, ongoing deficiencies, or deficiencies that are likely to or may occur in the future. With respect to the term "assess," the NOPR stated that NERC does not explain the scope of activities that are implied in the term "assess," which could range from a cursory review of an isolated "deficiency" to a detailed root-cause analysis. With respect to the term

"correct," the NOPR explained that NERC did not define what it means for a responsible entity to "correct" a deficiency. The NOPR stated that this term may include ending a deficiency, taking measures to address the effect of a deficiency, or taking steps to prevent a deficiency from recurring. With respect to the term "deficiency," the NOPR noted that NERC does not explain, nor does the text of the CIP version 5 Standards define, the term. The Commission observed that it is not clear whether "deficiencies" means "possible violations," as defined in NERC's Compliance Monitoring and Enforcement Program, or extends to a broader category of matters. The NOPR sought comment on these concerns and on any modification that may be necessary to address them.

48. The NOPR stated that the petition does not identify a reasonable timeframe for identifying, assessing and correcting deficiencies. Without identifying a timeframe, the NOPR explained that it is conceivable that, as long as the responsible entity identifies, assesses and corrects a deficiency before, or perhaps even when, NERC, the Regional Entities or the Commission discover the deficiency, there is no possible violation of the CIP Reliability Standards, regardless of the seriousness of the deficiency, the duration of the deficiency, or the length of time between the identification and correction of the deficiency. The NOPR sought comment on this concern and on any modifications that may be necessary to address it.

49. The NOPR stated that the proposed "identify, assess, and correct" language allows a responsible entity to avoid audit risk. The NOPR explained that, without a required timeframe for identifying, assessing and correcting a deficiency, a responsible entity

could defer its required assessment of its CIP compliance program until just prior to a scheduled audit or self-certification. The NOPR stated that NERC does not explain whether a responsible entity is required to disclose the identified deficiencies in such cases, and it is not clear whether the audit team can identify a potential violation if the responsible entity identifies the deficiency and is in the process of assessing and correcting it, even if the deficiency is identified long after it came into existence. The NOPR observed that it is also not clear how prior deficiencies that are identified, assessed and corrected are treated in assessing a responsible entity's compliance history. The NOPR sought comment on these concerns and on any modifications that may be necessary to address them.

50. The NOPR stated that the petition does not explain how NERC will treat multiple corrections of deficiencies concerning the same requirement, or the quality of the mitigation. The NOPR explained that it is unclear whether previous corrections will be reported or otherwise made known to NERC because they are not considered potential violations of the CIP Reliability Standard. The NOPR sought comment on this concern and on any modifications that may be necessary to address it.

51. In the NOPR, the Commission questioned how performance of the "identify, assess, and correct" language can be uniform or consistent among responsible entities absent clarification of Regional Entity and NERC compliance techniques.

52. The NOPR stated that neither the CIP version 5 Standards nor NERC's petition explain what is expected of responsible entities under the proposed "identify, assess, and correct" language. The NOPR expressed concern that including the assess and monitor

processes in the language of a requirement, as proposed by NERC, could render such requirements unenforceable. The NOPR sought comment on this concern and on any modifications that may be necessary to address them.

Comments

53. NERC comments that the Commission should approve the "identify, assess, and correct" language without modification. NERC explains that the "identify, assess, and correct" language is meant to address "frequently occurring security obligations (High Frequency Security Obligations) that present a lesser risk to reliability that reduces the administrative burden of the compliance process."[52] According to NERC, the intent of the "identify, assess, and correct" language is not to eliminate accountability for responsible entities or hinder Regional Entity, NERC or Commission oversight. NERC states that, if the "identify, assess, and correct" language is approved, it will submit a compliance filing by June 1, 2014 or six months from the date of the final rule in this docket, whichever is later, that "further outlines the compliance and enforcement aspects of this language, including when entities are expected to self-report or maintain documentation of its self-correcting process for audit, what constitutes potential noncompliance, and the necessary guidance for auditors."[53]

[52] NERC Comments at 5.

[53] *Id.* at 14.

54. NERC explains that the standard drafting team set out "to minimize the compliance burdens associated with High Frequency Security Obligations."[54] NERC contends that modifying or removing the "identify, assess, and correct" language through the NERC standard development process could delay implementation of the CIP version 5 Standards because the standard drafting team will have to consider alternative approaches. If the Commission directs removal or modifications to the "identify, assess, and correct" language, NERC states that the Commission should allow a reasonable time to develop changes through NERC's standard development process.

55. According to NERC, the "identify, assess, and correct" language is "intended to prescribe the manner in which entities must implement their policies and procedures for specific areas of security protection."[55] NERC claims that the best approach to address High Frequency Security Obligations is to "focus entities on correcting identified deficiencies in [the] implementation of the Technical Parts of the proposed requirements to promote continuous awareness in an entity's cyber security program."[56]

56. NERC distinguishes requirements containing the "identify, assess, and correct language" from other requirements. For requirements lacking the "identify, assess, and correct" language, NERC explains that responsible entities are "obligated to: (1) have the

[54] *Id.* at 7.

[55] *Id.* at 8.

[56] *Id.*

documented processes stated in the requirement, and (2) implement the documented processes to achieve the Technical Parts."[57] NERC comments that "[h]ow the entity chooses to implement the process would be documented for the Compliance Enforcement Authority, as required by the associated Measure … [f]or these requirements, the entity either has the process in place and the process achieves the Technical Parts or the entity does not have a process in place and/or its process does not achieve the Technical Parts."[58]

57. For requirements including the "identify, assess, and correct" language, NERC states that the "'identify, assess, and correct language' … mandates that the entity use a self-correcting process in its implementation of its documented policies to achieve the Technical Parts." NERC opines that the "self-correcting language does not affect the underlying obligation in the requirement to achieve the Technical Parts."[59] According to NERC, the only difference is that the "identify, assess, and correct" language "set[s] additional parameters for the manner in which an entity should implement the process."[60] NERC states, therefore, that the CIP version 5 Standards impose two obligations upon responsible entities. According to NERC, the CIP version 5 Standards that require a

[57] *Id.* at 9.

[58] *Id.*

[59] *Id.*

[60] *Id.* at 9-10.

documented process, regardless of whether such requirement includes the "identify, assess and correct" language, contain two obligations. The first requirement is to have the process mandated by the Reliability Standards and the second is the implementation of that process.

58. NERC contends that specifying a uniform definition of 'identify,' 'assess,' and 'correct' is impracticable given the wide range of systems and the number of assets that make up an entity's systems. NERC explains that the standard drafting team did not create specific definitions "because responsible entities are in the best position to define their own internal compliance processes based on the particular characteristics and make-up of their systems, including whether they will use internal controls or a different type of compliance management process to meet their specific system design."[61] According to NERC, if actual experience shows that an entity's compliance program does not meet compliance expectations, the "identify, assess, and correct" language mandates that the entity's processes and implementation be modified to correct any deficiencies. In addition, NERC states that, depending on the circumstances, "there may be a potential violation if actual performance does not meet the Technical Parts."[62]

59. NERC contends that the "identify, assess, and correct" language does not remove accountability for responsible entities, nor does it eliminate Regional Entity, NERC, and

[61] *Id.* at 10.

[62] *Id.* at 12.

Commission oversight. NERC claims that, by requiring responsible entities to demonstrate how their "identify, assess, and correct" process works, auditors will better understand a responsible entity's compliance program. NERC states that it is committed to developing Reliability Standard Audit Worksheets (RSAWs) and other guidance to support the adoption of the "identify, assess, and correct" language.

60. According to NERC, the term "deficiencies," as used in the sample RSAW, "referred to potential noncompliance with the proposed CIP Version 5 requirement; however not all deficiencies would be treated as possible violations depending on the specific facts and circumstances surrounding a deficiency."[63] NERC explains that a responsible entity would be expected to document the identification, assessment, and correction of lesser risk deficiencies for review by the Compliance Enforcement Authority, but that responsible entities would still be expected to self-report higher risk deficiencies. NERC comments that not requiring the individual reporting of lesser risk deficiencies will result in resource savings and allow entities to focus on security as opposed to the administrative aspects of the compliance process.

61. Regarding the timelines governing the "identify, assess, and correct" process, NERC states that "an entity's own internal processes would dictate the timing aspect."[64] NERC explains that a responsible entity would be required to explain the timing of its

[63] *Id.*

[64] *Id.* at 16.

process as part of an audit, and timing would be one factor in the auditors review of the entity's "identify, assess, and correct" process. Comparing the "identify, assess, and correct" language to the NIST Risk Management Framework, NERC opines that "requiring entities to continuously demonstrate that they are implementing processes in a manner that identifies, assesses, and corrects, is similar to the monitoring steps of the NIST Framework."[65]

62. Numerous commenters support the "identify, assess, and correct" language and do not indicate that there is a need for clarification.[66] These commenters assert that the "identify, assess, and correct" language is an improvement over the "zero tolerance" compliance approach in prior versions of the CIP Reliability Standards. The commenters also note that the "identify, assess, and correct" language was only added to requirements addressing lower risks to the reliability of the Bulk-Power System. For example, NextEra comments that "identify, assess, and correct" language is only found in requirements that "involve management of high volumes of information or data and those that involve execution of regular, periodic tasks. These are areas where scale matters; where, for example, one mistake out of thousands of non-mistakes does not necessarily

[65] *Id.* at 17.

[66] Alliant, AEP, APPA, Arkansas, SWP, Dominion, G&T Cooperatives, LADWP, MidAmerican, NARUC, OEVC, PG&E, PPL Companies, SCE, Tacoma, Tampa, TAPS, UI.

warrant the time and attention that must, by law, be given to 'potential violations' of a NERC reliability standard approved under Section 215 of the FPA."[67]

63. Commenters, including LADWP and Tacoma Power, claim that the "identify, assess, and correct" language is clear and creates incentives for responsible entities to improve internal controls to discover, evaluate, and address deficiencies.[68] The commenters assert that the "identify, assess, and correct" language could result in improved, more cost-effective reliability. The commenters generally disagree with the NOPR's concerns regarding the "identify, assess, and correct" language. For example, in response to the NOPR's concerns regarding timelines for completing "identify, assess, and correct" activities, MidAmerican states that "[a]ny time constraint on entities' remediation of discovered deficiencies would introduce another layer of required monitoring in areas where the industry has determined that ministerial compliance tasks are already unduly burdensome and counter-productive to the need to focus entities' limited resources on the most critical risks."[69]

64. Many commenters support retaining the "identify, assess, and correct" language in the requirements, but acknowledge the need for greater clarity as to how the "identify,

[67] NextEra Comments at 6.

[68] LADWP Comments at 8-9; Tacoma Power Comments at 2.

[69] MidAmerican Comments at 10.

assess, and correct" language will work in practice. [70] EEI and other commenters support NERC's proposal to submit a compliance filing that provides more detail regarding the "identify, assess, and correct" language. BPA, ISO New England and other commenters support allowing NERC to clarify the "identify, assess, and correct" language in a separate document in order not to delay implementation of the beneficial technical requirements in the CIP version 5 Standards.

65. Some commenters support modifying or removing the "identify, assess, and correct" language.[71] These commenters question whether the "identify, assess, and correct" language is auditable and enforceable due to a lack of clarity. While SPP RE comments that the "zero-defect" compliance aspect of the CIP Version 3 Reliability Standards is problematic, SPP RE also believes that the "identify, assess, and correct" language is unclear, subject to multiple interpretations, and difficult to audit.[72] TVA believes that it is imperative that the CIP standards, whose violations must necessarily be described generally at high levels, must be sufficiently clear in terms of what requirements are being imposed on Registered Entities and the "identify, assess, and

[70] Ameren, BPA, EEI, EPSA, Exelon, FirstEnergy, Idaho Power, ITC, ISO New England, KCP&L, Luminant, MISO, NASUCA National Grid, NRECA, NextEra, NAGF, Northeast Utilities, NorthWestern, Portland, Southern Indiana, Wisconsin, Xcel.

[71] Encari, GSOC, SPP Parties, SCE&G, SPP RE, and TVA.

[72] SPP RE Comments at 2-3.

correct" language is too vague to ascertain how compliance will be audited.[73] While SCE&G favors retaining the "identify, assess, and correct" concept, SCE&G also contends that it is misplaced in NERC's proposed CIP version 5 Standards where it is embedded in the technical parts of the requirements.[74]

66. Commenters express differing views on the obligations imposed by the "identify, assess, and correct" language irrespective of their position on whether that language should be retained. For example, MISO indicates that the "identify, assess, and correct" language could be interpreted as imposing a new obligation or not imposing a new obligation on responsible entities.[75] MidAmerican and Luminant assert that the "identify, assess, and correct" language would not impose a new compliance obligation. However, according to LADWP and OEVC, the "identify, assess, and correct" language would impose a new obligation (i.e., to have an "identify, assess, and correct" process in place). Other commenters, including GSOC and ITC, ask the Commission to clarify that the "identify, assess, and correct" language cannot be separately violated and that only a failure to comply with the underlying substantive requirement can result in a violation.

[73] TVA Comments at 2-3.

[74] SCE&G Comments at 2.

[75] MISO Comments at 4.

Commission Determination

67. For the reasons discussed below, the Commission concludes that the "identify, assess, and correct" language, as currently proposed by NERC, is unclear with respect to the obligations it imposes on responsible entities, how it would be implemented by responsible entities, and how it would be enforced. Accordingly, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements, while retaining the substantive provisions of those requirements.[76] Alternatively, NERC may propose equally efficient and effective modifications that address the Commission's concerns regarding the "identify, assess, and correct" language.[77] The Commission directs NERC to submit the modifications to the CIP Reliability Standards within one year from the effective date of this Final Rule.

68. In Order No. 672, the Commission provided general guidance on the conditions under which a Reliability Standard would be approved under Section 215 of the Federal

[76] The 17 requirements are: CIP-003-5, Requirements R2 and R4; CIP-004-5, Requirements R2 through R5; CIP-006-5 Requirements R1 and R2; CIP-007-5, Requirements R1 through R5; CIP-009-5, Requirement R2; CIP-010-1, Requirements R1 and R2; and CIP-011-1, Requirement R1.

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

Power Act.[78] Among other things, the Commission explained that proposed Reliability Standards should be clear and unambiguous regarding what is required for compliance and who is required to comply.[79] Based on our experience with the ongoing development and implementation of the Reliability Standards, including the CIP Reliability Standards, we believe that clarity and certainty in the language of Reliability Standard requirements is necessary to ensure consistent application by responsible entities, as well as consistent enforcement by NERC and the Regional Entities.[80] Language in a requirement that could be subject to multiple interpretations raises the specter of inconsistent application and enforcement, which could result in risks to Bulk-Power System reliability.[81] Therefore, as a fundamental expectation, NERC must strive to develop clear and unambiguous Reliability Standards .

69. As we indicated in the NOPR, we support NERC's move away from a "zero tolerance" approach to compliance, the development of strong internal controls by responsible entities, and NERC's development of standards that focus on the activities

[78] Order No. 672, FERC Stats. & Regs. ¶ 31,204 at PP 320-337.

[79] *Id.* P 325.

[80] *See id.* P 327 (stating that a proposed Reliability Standard should include "a clear criterion or measure of whether an entity is in compliance" and should "contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.").

[81] *See* Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 274 (finding that "it is essential that the Requirements for each Reliability Standard . . . are sufficiently clear and not subject to multiple interpretations.").

that have the greatest impact on Bulk-Power System reliability.[82] Thus, we are sympathetic to these underlying motives as described by NERC that resulted in the incorporation of the "identify, assess, and correct" language within 17 provisions of the CIP version 5 Standards. Nonetheless, as explained below, the language proposed by NERC is ambiguous and results in an unacceptable amount of uncertainty with regard to consistent application, responsible entities understanding their obligations, and NERC and the regions providing consistent application in audits and other compliance settings.

70. The Commission raised concerns in the NOPR with the "identify, assess, and correct" language and sought comment on the implementation and enforceability of the "identify, assess, and correct" language. The commenters, however, do not clarify how the "identify, assess, and correct" language would be implemented and enforced. Rather, the diversity of explanations provided by commenters reinforces our concerns. In its petition and comments, NERC does not clarify adequately the language and, instead, indicates that it is willing to submit a future compliance filing that "further outlines the compliance and enforcement aspects of this language, including when entities are expected to self-report or maintain documentation of its self-correcting process for audit, what constitutes potential noncompliance, and the necessary guidance for auditors."[83] NERC's proposal that the Commission approve this language in numerous requirements

[82] *See* NOPR, 143 FERC ¶ 61,055 at P 57.

[83] NERC Comments at 14.

of the CIP version 5 Standards, while postponing a detailed explanation regarding the understanding, compliance implications and proper implementation of the proposed language to a future time, is an inadequate approach.

71. Moreover, there is confusion among the commenters as to what the "identify, assess, and correct" language requires of responsible entities. For example, commenters differ on whether the "identify, assess, and correct" language imposes a new obligation on responsible entities. The Commission raised questions in the NOPR concerning, among other things, reasonable timeframes for identifying and correcting a deficiency, whether the language could be used to avoid audit risk, and how the implementation and performance of the language can be expected to be consistent across responsible entities and regions, but did not receive adequate responses.[84] We received inconsistent explanations in response to these inquiries, which we take as another indication of the vagueness of the "identify, assess, and correct" language.

72. Regarding the meaning of the terms "identify," "assess," "correct," and "deficiencies," NERC states that it would be impracticable to develop uniform definitions and that responsible entities are in the best position to define these terms in the context of their internal compliance programs. While we understand NERC's desire to allow for flexibility as responsible entities develop their internal control programs, we are, nonetheless, concerned that the NERC proposal lacks basic definition and guidance that

[84] *See* NOPR, 143 FERC ¶ 61,055 at PP 51, 52, and 54.

is needed, for example, to distinguish a successful internal control program from one that is inadequate. As a result, we conclude that the "identify, assess, and correct" language, as currently proposed, injects an unacceptable degree of ambiguity into the otherwise reasonable substantive requirements of the CIP version 5 Standards.

73. As indicated earlier, we support the underlying concerns that prompted the "identify, assess and correct" language, namely encouraging the development of strong internal controls and focusing resources on activities that best promote reliability of the Bulk-Power System. We believe, however, that it may be more appropriate for NERC to achieve these goals by articulating defined goals in the compliance and enforcement process and identifying clear expectations that would justify the exercise of enforcement discretion. For example, the Reliability Assurance Initiative process when fully developed may afford a consistent, informed approach that provides incentives for entities to develop robust internal control programs.[85]

74. We emphasize that if NERC wishes to propose modifications other than, or in addition to, removing the "identify, assess and correct" language from the CIP version 5 requirements, we will be open to consideration of various approaches for resolving the High Frequency Security Obligations scenario NERC identifies. We understand the concern to be that while it is necessary for Bulk-Power System reliability to identify,

[85] The Reliability Assurance Initiative program is a NERC initiative to transform the current compliance and enforcement program into one that focuses on high reliability risk areas and reduces the administrative burden on registered entities. *See* http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

control, and minimize violations of requirements addressing this scenario, responsible entities may not be able to prevent all such violations. Moreover, while it is possible that a single violation of such a requirement could result in significant harm to Bulk-Power System reliability, or that multiple or repeated violations by an individual responsible entity could indicate a reliability vulnerability or inadequate internal controls, individual violations of such requirements likely pose a low risk. With respect to these types of requirements, we are receptive to the concept that Bulk-Power System reliability may be better served, at lower cost to responsible entities, for Regional Entities and NERC to provide incentives for them to proactively identify and mitigate potential noncompliance outside the enforcement context by enhancing their internal controls.

75. 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.

76. Accordingly, the Commission directs NERC, pursuant to section 215(d)(5) of the FPA, to develop modifications to the CIP version 5 Standards that address our concerns. Preferably, NERC should remove the "identify, assess, and correct" language from the 17 CIP version 5 requirements. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this Final Rule. Alternatively, NERC may develop a proposal to enhance the enforcement discretion afforded to itself and the Regional Entities, as discussed above.

B. BES Cyber Asset Categorization and Protection

1. Reliability Based Criteria

NERC Petition

77. Reliability Standard CIP-002-5 requires responsible entities to categorize BES Cyber Systems as having a Low, Medium, or High Impact. NERC states that CIP-002-5 requires "the identification and categorization of BES Cyber Systems according to specific criteria that characterize their impact for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the [bulk electric system]."[86] NERC states that the new approach to classifying cyber systems, which

[86] NERC Petition at 11.

requires a minimum classification of "Low Impact" for all BES Cyber Systems, "resulted from a review of the NIST Risk Management Framework for categorizing and applying security controls, a review that was directed by the Commission in Order No. 706."[87]

NOPR

78. In the NOPR, the Commission pointed out that NERC's proposed categorization process is based on facility ratings, such as generation capacity and voltage levels, whereas the NIST Risk Management Framework categorizes systems based on cyber security principles regarding the confidentiality, integrity, and availability of systems.[88] The Commission stated in the NOPR that NERC's new approach to categorizing BES Cyber Systems, which requires at least a minimum classification of "Low Impact" for all BES Cyber System, is a step closer to comprehensively protecting assets that could cause cyber security risks to the bulk electric system.[89] The Commission proposed to accept NERC's proposal, recognizing that the Commission may revisit the categorization of assets under the CIP Reliability Standards at a later date should the need arise.[90]

[87] *Id.* at 15.

[88] NOPR, 143 FERC ¶ 61,055 at P 61.

[89] *Id.* P 59.

[90] *Id.* P 64.

Comments

79. The commenters generally support the proposed bulk electric system categorization process, with some commenters raisings discrete concerns with certain aspects of the NOPR.

80. NERC, BPA, and CenterPoint support the proposed categorization process. NERC states that the proposed Low, Medium, or High Impact categories were derived from a review of the NIST Risk Management Framework conducted in response to the Commission's directive in Order No. 706.[91] NERC explains that, based on the review of the NIST Risk Management Framework, the standard drafting team determined that a Low, Medium, or High Impact categorization based on facility ratings is appropriate "because it (1) reflects the well understood and commonly used method for categorizing assets within the electricity sector; (2) provides a clear and measurable method for identifying assets; and (3) directly relates to a facility's impact on the Bulk Electric System, which is consistent with the NIST Framework approach to categorizing assets based on risk."[92]

81. NERC, BPA and CenterPoint comment that, although the proposed reliability-based criteria put forth in CIP version 5 differ from the NIST Risk Management Framework, where the categorization process is based on the loss of confidentiality,

[91] BPA Comments at 6; CenterPoint Comments at 2-3; NERC Comments at 18-19.

[92] NERC Comments at 18-19.

integrity, and availability systems, the difference is reasonable. Specifically, NERC, BPA and CenterPoint note that the NIST standards are information protection standards whereas the CIP Standards are reliability standards, which require a slightly different approach to categorization aimed more broadly at the reliability of the Bulk-Power System across all entities rather than categorization by a single organization.[93]

82. TVA states that it "would be in favor of transitioning to a NIST categorization model if the control scoping and implementation was conducted in accordance with NIST-800-37, revision 1."[94] TVA asserts that the NIST Risk Management Framework, if applied correctly, provides near real time management of risks, and establishes responsibility and accountability for information system security. TVA concludes that the NIST Risk Management Framework "has the potential to provide the utility industry with a proven and effective security framework that includes targeted components uniquely written for the control system environment."[95]

83. ITC states that blackstart resources, which are designated as Low Impact under proposed CIP-002-5, should be designated as Medium Impact assets to ensure sufficient protection of the bulk electric system.[96] ITC states that blackstart resources are of similar

---

[93] NERC Comments at 19; BPA Comments at 6; CenterPoint Comments at 2-3.

[94] TVA Comments at 4.

[95] *Id.*

[96] ITC Comments at 8.

importance as other assets designated as Medium Impact and, therefore, blackstart resources should be protected as such, including the appropriate VRF designation.[97] ITC avers that blackstart resources "are analogous to Criteria 2.3 generation resources because they are necessary to avoid an Adverse Reliability Impact as defined by NERC, and should therefore be classified as Medium Impact."[98] ITC contends that NERC's rationale for classifying blackstart resources as Low Impact assets is faulty. Specifically, ITC argues that classifying blackstart resources as Low Impact "because of concerns over additional compliance costs leading to withdrawal of Blackstart resources from the market" is not an appropriate rationale for approving a reliability rule.[99]

84. SPP RE asserts that the proposed categorization process fails to address connectivity as directed in Order No. 761. Specifically, SPP RE notes that the Commission directed NERC to "address a cyber asset's connectivity and its potential to compromise the reliable operation of the Bulk-Power System with respect to the BES Cyber Asset categorization criteria."[100] SPP RE recommends that the Commission direct NERC to modify the BES Cyber Asset categorization process "to require control centers performing the functional obligations of Balancing Authority or Generation Operator to

[97] *Id.*

[98] *Id.* at 9.

[99] *Id.*

[100] SPP RE Comments at 5 (citing Order No. 761, 139 FERC ¶ 61,058 at P 91).

be categorized as medium impact at a minimum if the control center systems are network interconnected" with other control center systems.[101]

85. Tampa seeks clarification concerning the CIP-002-5, Attachment 1 impact rating criteria as they relate to certain generating units. Specifically, Tampa requests clarification "whether individual units less that 20 MVA (gross nameplate rating) and generating plants/facilities less than 75 MVA (gross aggregate nameplate rating) are excluded from consideration as Low Impact assets."[102] Tampa questions whether there is a criterion that would qualify a generation facility as Low Impact besides failing to meet the two criteria that qualify a facility as Medium Impact, or are all remaining generation facilities captured by the Low Impact definition. Tampa also questions whether the bulk electric system definition acts as a floor for Low Impact facilities under which Low Impact facilities would not include facilities that are excluded from the definition of the bulk electric system. Tampa requests that the Commission clarify that only those generation facilities equal to or greater than 1500 MW or that are designated by either a planning coordinator or transmission planner will be considered Medium Impact, with all remaining generating facilities considered Low Impact, subject to any bulk electric system definition floor.[103]

---

[101] *Id* at 6.

[102] Tampa Comments at 4.

[103] *Id.*

86. Wisconsin questions the applicability section of the proposed CIP version 5 Standards. Specifically, Wisconsin asserts that the CIP version 5 Standards, as written, could be read to exclude reliability coordinators and other entities from the CIP Standards because section 4.2.2 in each of the CIP Standards limits applicability to a responsible entity's bulk electric system facilities. Wisconsin notes that neither reliability coordinators nor interchange authorities have bulk electric system facilities. Wisconsin requests that the Commission require NERC to remove section 4.2.2 from each of the CIP Standards to ensure that the standards are clear and unambiguous with regard to applicability.[104]

Commission Determination

87. The Commission finds reasonable the categorization of BES Cyber Systems set forth in Reliability Standard CIP-002-5. The new approach to categorizing BES Cyber Systems, 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. The Commission may revisit the categorization of BES Cyber Assets should experience gained from implementing and enforcing Reliability Standard CIP-002-5 warrant such action.

88. With regard to ITC's comments on blackstart resources, we are not persuaded that blackstart resources should be designated as Medium Impact BES Cyber Assets. While

[104] Wisconsin Comments at 4.

we believe that system recovery is important to the reliable operation of the Bulk-Power System, we accept the ERO's approach on this matter as adequate. Further, since blackstart resources are designated as Low Impact, entities may have discretion regarding appropriate security controls that will apply. Although we determine not to direct changes at this time, we may revisit this determination after implementation of the CIP version 5 Standards if we determine that blackstart resources lack a sufficient level of protection. ITC is also encouraged to raise its concerns regarding blackstart resources through NERC's standards development process.

89. With respect to SPP RE's concerns on the issue of connectivity, the Commission does not direct changes at this time. The majority of bulk electric system control centers are designated as High Impact BES Cyber Assets under Reliability Standard CIP-002-5 because of the interconnected nature of these facilities. We share SPP RE's concern, however, that balancing authority and generation operator control centers are interconnected and some of these facilities will likely fall into the Low Impact category. The Commission may revisit this determination if we find that Low Impact control centers lack a sufficient level of protection following implementation of the CIP version 5 Standards.

90. As noted above, Tampa requests clarification concerning the CIP-002-5 impact rating criteria as it relates to certain generating units. The Commission clarifies that, consistent with our determinations in Order No. 773, only those plants, facilities, and assets that are covered under the bulk electric system definition, or included in the definition under the exceptions process in Appendix 5C of the NERC rules of procedure,

will be required to comply with the CIP Reliability Standards.[105] Similarly, the Low Impact category will not include assets that are not covered under the bulk electric system definition or excluded from the definition under the exceptions process in Appendix 5C of the NERC rules of procedure. The Commission understands that the Low Impact category is intended to address all BES Cyber Systems on the bulk electric system that do not meet the criteria for Medium or High Impact.

91. With respect to Wisconsin's comments, we do not agree that section 4.2.2 excludes reliability coordinators and interchange authorities from the CIP Reliability Standards as the facilities associated with both classes of entities can be accurately described as BES Cyber Systems under the NERC glossary. Section 4.1 of the applicability section of CIP-002-5 explicitly identifies reliability coordinators (section 4.1.6) and interchange authorities (section 4.1.5) as applicable entities. Section 4.2 of the Reliability Standard identifies the "Facilities, systems and equipment" owned by responsible entities "to which these requirements [of CIP-002-5] are applicable," and section 4.2.2 provides that for all entities other than distribution providers, the applicable facilities are "[a]ll BES Facilities." In Order No. 773, we determined that the term "bulk electric system" incorporates "associated equipment" that broadly includes facilities such

[105] *Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure*, Order No. 773, 141 FERC ¶ 61,236, at P 43 (2012) (noting that "[t]he [bulk electric system] definition, coupled with the exception process will ensure that facilities not necessary for the operation of the interconnected transmission network will be properly categorized."), *order on reh'g*, Order No. 773-A, 143 FERC ¶ 61,053, *order denying clarification*, 144 FERC ¶ 61,174 (2013).

as control centers and other assets.[106] We are satisfied that the CIP version 5 Standards explicitly apply to reliability coordinators and interchange authorities and that they are not precluded from having applicable facilities based on the language of the standards.

92. According to NERC, development of the BES Cyber System categorization process included a review of the NIST Risk Management Framework.[107] There is a significant distinction, however, between NERC's categorization process and the NIST Risk Management Framework. In particular, NERC's categorization process is based on facility ratings, such as generation capacity and voltage levels.[108] In contrast, the NIST Risk Management Framework categorizes systems based on cyber security principles regarding the confidentiality, integrity, and availability of systems. Commenters such as NERC and BPA aver that such differences are reasonable and justified because the NIST standards are information protection standards whereas the CIP Standards are reliability standards, aimed more broadly at the reliability of the Bulk-Power System across all entities rather than categorization by a single organization. We find this explanation to be reasonable and, therefore, we do not direct any modifications regarding the BES Cyber System categorization process in Reliability Standard CIP-002-5 at this time.

---

[106] Order No. 773, 141 FERC ¶ 61,236 at P 53 (noting that "core [bulk electric system] definition also continues to capture equipment associated with the facilities included in the bulk electric system.").

[107] *See* NERC Petition at 31.

[108] *See* NOPR at, 143 FERC ¶ 61,055 P 63.

However, as discussed below, the NIST Risk Management Framework, as well as other issues relating to the CIP Reliability Standards, will be the subject of a future staff-led technical conference.

2. Protection of Low Impact BES Cyber Assets

NERC Petition

93. Reliability Standard CIP-003-5, Requirement R2, which pertains to the obligations for BES Cyber Systems identified as Low Impact, provides:

> R2. Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3 [i.e., low impact systems], 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.
> An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

This is the only CIP version 5 requirement applicable to Low Impact systems.

NOPR

94. In the NOPR, the Commission expressed concern with Requirement R2 of Reliability Standard CIP-003-5, which requires responsible entities to "implement … documented cyber security policies" that address: (1) cyber security awareness, (2) physical security controls, (3) electronic access controls and (4) incident response to a cyber security incident. The NOPR explained that Requirement R2 sets forth the single

compliance obligation for BES Cyber Systems categorized as Low Impact.[109] The Commission expressed concern that NERC's proposal to limit the protections for Low Impact BES Cyber Systems to documented policies, as opposed to requiring specific cyber security protections, could result in ambiguities that lead to inconsistent and inefficient implementation of the CIP Reliability Standards with regard to Low Impact BES Cyber Systems and may not provide an adequate roadmap for responsible entities to follow to ensure the reliable operation of the bulk electric system.[110]

95. The NOPR proposed to direct that NERC develop a modification to CIP-003-5, Requirement R2, to require responsible entities to adopt specific, technically-supported cyber security controls for Low Impact assets, as opposed to the proposed unspecified policies.[111] The NOPR sought comment on (1) the value of adopting specific controls for Low Impact assets that reflect their cyber security risk level and (2) the lack of a requirement to have an inventory, list or discrete identification of Low Impact BES Cyber Systems.

---

[109] NOPR, 143 FERC ¶ 61,055 at P 66.

[110] *Id.* P 70.

[111] *Id.*

Comments

Low Impact Protections

96. The majority of commenters oppose the Commission proposal to require entities to adopt specific cyber security controls for Low Impact assets and support CIP-003-5, Requirement R2 as filed. Other commenters support NERC's proposal, but also believe that additional guidance regarding the protection of Low Impact assets would be beneficial. Several commenters do not support NERC's proposal on Low Impact assets, but not based on the concerns raised in the NOPR.

97. The majority of commenters support proposed CIP-003-5, Requirement R2 as filed and oppose the NOPR proposal to require specific, technically-supported controls for Low Impact BES Cyber Assets.[112] Generally, commenters state that the CIP-003-5, Requirement R2 requirement for responsible entities to develop and implement documented cyber security policies is appropriate for assets that will be categorized as having a limited effect on the bulk electric system. NERC characterizes the requirement to develop and implement cyber security policies for Low Impact assets as "a significant

[112] *See, e.g.*, Comments of Alliant, Ameren, AEP, APPA, Arkansas, BPA, CenterPoint, Consumers Energy, Dominion, EEI, Holland, Idaho Power, ISO New England, Luminant, MidAmerican, NARUC, National Grid, NRECA, NextEra, NERC, NAGF, Northeast Utilities, NIPSCO, PG&E, Pepco, Portland, PPL Companies, Southern Indiana, SWP, Tacoma, Tampa, TVA, TAPS, UI, Xcel.

step in more comprehensively protecting assets that could cause cyber security risks to the bulk electric system."[113]

98. EEI asserts that the proposed protections for Low Impact assets include basic physical and electronic perimeter-type access controls for every bulk electric system facility housing any BES Cyber Asset, including Low Impact assets.[114] CenterPoint, Consumers Energy, and Holland comment that CIP-003-5, Requirement R2 establishes an auditable requirement that responsible entities develop and implement cyber security policies covering the four areas identified in Requirement R2.

99. APPA, Holland and others, comment that requiring responsible entities to adopt specific cyber security controls for Low Impact BES Cyber Systems would significantly increase the cost and administrative burden associated with the protection of Low Impact BES Cyber Systems with little to no increase in bulk electric system reliability.[115] NextEra, among other commenters, asserts that a requirement to adopt specific, technically-supported controls for Low Impact BES Cyber Systems would take time and resources away from the protection of Medium and High Impact BES Cyber Systems.[116]

---

[113] NERC Comments at 21.

[114] EEI Comments at 13-14.

[115] *E.g.*, APPA Comments at 14; SWP Comments at 5; Consumers Energy Comments at 3; Idaho Power Comments at 2-3; NARUC Comments at 5-6; NRECA Comments at 8-9; PHI Comments at 4; SCE Comments at 4; TAPS Comments at 4.

[116] NextEra Comments at 5; Alliant Comments at 5; EEI Comments at 14; KCP&L Comments at 4; NRECA Comments at 8-9.

ISO New England raises a concern that adopting a new requirement for specific controls for Low Impact assets could have unintended consequences, such as the withdrawal of blackstart resources.[117]

100. Some comments oppose the NOPR proposal to require specific, technically-supported controls for Low Impact BES Cyber Assets, but acknowledge that additional guidance regarding the protection of Low Impact assets would be beneficial.[118] Specifically, SPP Parties, LADWP and KCP&L posit that additional guidance would aid responsible entities in understanding what security measures they should adopt for Low Impact assets, as well as help ensure that audit requirements are clear. AEP suggests that, if the Commission directs NERC to require prescriptive controls for Low Impact assets, such requirements should include a caveat that the controls will only be implemented where technically feasible.

101. OEVC and SPP RE do not support proposed CIP-003-5, Requirement R2, but for different reasons. OEVC states that the category of Low Impact BES Cyber Assets is flawed because it encompasses entities that do not have an impact on the bulk electric system and, as such, exceeds the authority granted in FPA section 215.[119] SPP RE claims that only requiring documented policies that cover broadly-defined topics provides

---

[117] ISO New England Comments at 9.

[118] *E.g.*, SPP Parties Comments at 3; LADWP Comments at 11; KCP&L Comments at 4.

[119] OEVC Comments at 10.

insufficient protection for Low Impact BES Cyber Assets.[120] SPP RE comments that the failure to require specific controls is problematic for auditors in that CIP-003-5, Requirement R2 lacks specific control objectives with which to measure an entity's compliance. SPP RE recommends defining an appropriate set of control objectives as opposed to defining the controls themselves.[121]

102. NARUC raises a concern that the breadth of the Low Impact category has the potential to blur the clear jurisdictional lines in FPA section 215. NARUC concludes that a "lighter touch," such as NERC's proposed documented policies under CIP-003-5, Requirement R2, is the appropriate manner to address assets that by definition are low priority.[122]

Inventory of Low Impact Assets

103. The majority of commenters oppose adopting a requirement for responsible entities to develop and maintain an inventory, list or discrete identification of Low Impact BES Cyber Assets.[123] NERC, EEI, Idaho Power, NRECA, TVA, Xcel and others argue that developing and maintaining an inventory or list of Low Impact assets would create

[120] SPP RE Comments at 6.

[121] *Id.* at 7-8.

[122] NARUC Comments at 6.

[123] *See* Comments of Ameren, Arkansas, BPA, Consumers Energy, Dominion, EEI, Idaho Power, LADWP, Luminant, MidAmerican, NRECA, NERC, NAGF, NIPSCO, PG&E, PEPCO, SCE, SPP Parties, Tampa, TVA, UI, and Xcel.

an unnecessary administrative burden without any corresponding reliability benefit.[124] Luminant comments that a requirement to develop and maintain an inventory or list of Low Impact assets would be an administrative task that would create additional intelligence source data that must be protected.[125] EEI suggests that Low Impact assets should be identified at the site facility level and not the individual device level.[126]

104. According to NERC, no added reliability benefit would result from a separate requirement to create and continuously update a list of Low Impact assets. NERC notes, however, that CIP-002-5 Part 1.3 requires responsible entities to identify each bulk electric system asset that contains a Low Impact BES Cyber System and, therefore, responsible entities should have a list of bulk electric system locations containing Low Impact BES Cyber Systems that could be used for audit purposes.[127] In contrast, SPP RE states that the lack of a requirement for responsible entities to maintain an inventory of Low Impact BES Cyber Assets poses an audit challenge because neither the responsible

[124] *See also* Ameren Comments at 11; BPA Comments at 8; Consumers Energy Comments at 4; Dominion Comments at 10; SCE Comments at 4; SPP Parties at 3; Luminant Comments at 4; NAGF Comments at 4; PG&E Comments at 7; PHI Comments at 4; SCE Comments at 4; Tampa Comments at 5-6; and UI Comments at 6.

[125] Luminant Comments at 4.

[126] EEI Comments at 14-15.

[127] NERC Comments at 22-23.

entity nor the auditor will have a reasonable assurance that every BES Cyber System or BES Cyber Asset has been accounted for and properly categorized.[128]

105. LADWP supports removing the language from CIP-003-5, Requirement R2, stating that an inventory or list of Low Impact BES Cyber Systems or BES Cyber Assets is not required. LADWP agrees with the Commission that the process of identifying and categorizing assets into Low, Medium, and High Impact categories will lend itself to compiling a list or inventory of all BES Cyber Assets, including Low Impact assets. LADWP suggests that, since entities will already be maintaining a list for internal classification purposes, a requirement to maintain a list of Low Impact BES Cyber Assets would not impose additional burdens.[129]

Commission Determination

Specific Controls for Low Impact BES Cyber Systems

106. Based on the explanations provided by NERC and other commenters, we adopt the NOPR proposal with modifications. As we explain below, while we do not require NERC to develop specific controls for Low Impact facilities, we do require NERC to address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for Low Impact assets. While NERC

[128] SPP RE Comments at 7-8.

[129] LADWP Comments at 13.

may address this concern by developing specific controls for Low Impact facilities, it has the flexibility to address it through other means, including those discussed below.

107. As highlighted by commenters, the adoption of the Low Impact BES Cyber Asset category will expand the protections offered by the CIP version 5 Standards to additional assets that could cause cyber security risks to the bulk electric system. As discussed above, categorizing BES Cyber Systems based on their Low, Medium, or High Impact on the reliable operation of the bulk electric system, with all BES Cyber Systems being categorized as at least Low Impact, offers more comprehensive protection of the bulk electric system. The CIP version 5 Standards, however, do not require specific controls for Low Impact assets nor do they contain clear, objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities for Low Impact BES Cyber Systems.

108. In addition, the absence of objective criteria to evaluate the controls chosen by responsible entities for Low Impact assets introduces an unacceptable level of ambiguity and potential inconsistency into the compliance process, and creates an unnecessary gap in reliability. This ambiguity will make it difficult for registered 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. Therefore, pursuant to section 215(d)(5) of the FPA, we direct NERC to develop modifications to the CIP version 5 Standards to address this concern. We believe that NERC can effectively 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. We believe that this approach allows NERC the flexibility to develop appropriate modification(s), while also considering the stakeholder concerns expressed in NOPR comments regarding the possible rigidity of requiring a "one-size-fits-all" set of controls.

109. We disagree with OEVC's assertion that the Low Impact category is flawed because it applies to responsible entities that do not have an impact on the bulk electric system and, as such, exceeds the authority granted in FPA section 215. Reliability Standard CIP-002-5 encompasses cyber assets that meet the definition of a BES Cyber Asset and that are associated with facilities that are part of the bulk electric system.[130] Further, only those cyber assets that meet the definition of a BES Cyber Asset and are a part of a BES Cyber System must comply with the controls in the CIP Reliability

[130] *See* Reliability Standard CIP-002-5 (Cyber Security – BES Cyber System Categorization) at Section 3 (the stated purpose of CIP-002-5 is "[t]o identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the [bulk electric system].").

Standards. Accordingly, Low Impact assets fall within the scope of FPA section 215. While SPP RE raises concerns regarding the auditability of Reliability Standard CIP-003-5, Requirement R2, in the absence of specific control objectives, other commenters such as CenterPoint and Consumers Energy assert that Requirement R2 establishes an auditable requirement that responsible entities both develop and implement cyber security policies addressing the four identified areas. We believe that our directive to NERC will address any concerns over the auditability of the protections adopted under CIP-003-5, Requirement R2.

110. As discussed above, NERC has flexibility in how it addresses our concern. For example, NERC could follow the recommendation of SPP RE and define an appropriate set of control objectives for Low Impact assets, rather than define the specific controls that would apply to Low Impact assets. Alternatively, NERC may propose specific controls that apply to Low Impact assets, including subdividing the assets into different categories with different defined controls or control objectives applicable to each subcategory, or it could define with greater specificity the processes that responsible entities must have for Low Impact facilities under CIP-003-5, Requirement R2. NERC may also propose an alternative approach that addresses our concern in an equally efficient and effective manner. Whatever approach NERC decides to take, we emphasize that 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.

Inventories of Low Impact BES Cyber Systems

111. In the NOPR, the Commission sought comment on the benefit of requiring a list or inventory of Low Impact BES Cyber Systems.[131] Based on the comments, we are persuaded that it would be unduly burdensome to require responsible entities to create and maintain an inventory of Low Impact assets for audit purposes. Creating and maintaining such a list could also divert resources away from the protection of Medium and High Impact assets. Further, we note that NERC's approach is consistent with its move away from embedding documentation obligations in the substantive requirements of Reliability Standards.

112. We agree with NERC's comment that, while not requiring a list or inventory, "NERC stresses that entities will need to be able to demonstrate compliance with CIP-002-5, which requires such entities to identify the assets that are associated with its Low Impact BES Cyber Systems."[132] Thus, NERC indicates that, while not necessarily in the form of a discrete list, an entity must have the ability to identify the nature and location of all Low Impact assets that it owns or controls for audit and compliance purposes. Likewise, as explained by NERC, pursuant to Reliability Standard CIP-002-5, Requirement R1, Part 1.3, auditors have the ability to ensure that Low Impact systems are accounted for by confirming that a responsible entity has identified "each asset that

[131] *See* NOPR, 143 FERC ¶ 61,055 at P 71.

[132] NERC Comments at 22.

contains a low impact BES Cyber System[.]"[133] We find this explanation to be reasonable.

C. Proposed Definitions

113. In its petition, NERC proposes nineteen CIP-related definitions for inclusion in the NERC Glossary. This includes fifteen new definitions and four revised definitions, as well as the retirement of two definitions.[134] The NOPR proposed to approve the definitions for inclusion in the NERC Glossary. The NOPR also sought comment on certain aspects of the proposed definitions. The Commission stated in the NOPR that, depending on the adequacy of the explanations provided in response to the NOPR questions, the Commission may direct NERC to develop modifications to certain proposed definitions to eliminate ambiguities and ensure that BES Cyber Assets are adequately protected.

[133] Reliability Standard CIP-002-5 (Cyber Security – BES Cyber System Categorization), at Requirement 1, Part 1.3.

[134] Newly proposed definitions include BES Cyber Asset, BES Cyber System, BES Cyber System Information, CIP Exceptional Circumstances, CIP Senior Manager, Control Center, Dial-up Connectivity, Electronic Access Control or Monitoring Systems (EACMS), Electronic Access Point (EAP), External Routable Connectivity, Interactive Remote Access, Intermediate System, Physical Access Control Systems (PACS), Protected Cyber Assets (PCA), and Reportable Cyber Security Incident. Revised definitions include Cyber Assets, Cyber Security Incident, Electronic Security Perimeter (ESP), and Physical Security Perimeter (PSP). Retired definitions include Critical Assets and Critical Cyber Assets.

114. As discussed below, we approve the nineteen definitions. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop requirements that address issues raised by the definitions and to submit an informational filing.

1. Definition - BES Cyber Asset

NERC Petition

115. NERC proposes the following definition of a BES Cyber Asset:

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

a. 15-Minute Parameter

NOPR

116. The NOPR sought comment on the purpose and effect of the 15-minute parameter in the BES Cyber Asset definition. In particular, the NOPR sought comment on the types of Cyber Assets that would meet the "within 15 minutes" parameter.[135] Further, the NOPR sought comment on the types of assets or devices that the 15-minute parameter would exclude and, in particular, whether the "within 15 minutes" parameter excludes devices that have an impact on the reliable operation of the bulk electric system.[136] The NOPR also sought comment on whether the use of a specified time period as a basis for identifying assets for protection is consistent with the procedures adopted under other cyber security standards, such as the NIST Risk Management Framework, that apply to industrial control and Supervisory Control and Data Acquisition (SCADA) systems, as well as traditional information technology systems.[137]

[135] NOPR, 143 FERC ¶ 61,055 at P 77.

[136] *Id.*

[137] *Id.*

Comments

117. Most commenters support the 15-minute parameter,[138] stating that the 15-minute parameter is consistent with existing Commission-approved Reliability Standards. Other commenters contend that the 15-minute parameter is arbitrary and lacks justification.

118. NERC, AEP, EEI, Idaho Power and PPL state that the proposed 15-minute parameter provides a level of consistency for the identification of BES Cyber Assets that could have a real-time impact on the reliability of the bulk electric system.[139] Similarly, KCP&L and UI support the 15-minute parameter as a proxy for real-time operations, and KCP&L explains that the proposed definition should not automatically exempt any assets that have an impact on the reliable operation of the bulk electric system.[140]

119. NERC, Luminant, and MISO comment that the 15-minute parameter is consistent with Commission-approved reliability standards.[141] Luminant notes that 15-minute parameter is consistent with the disturbance recovery period under Reliability Standard BAL-002-1. NERC and MISO state that the Commission has previously approved the

[138] *E.g.*, Ameren, AEP, EEI, Idaho Power, KCP&L, Luminant, MidAmerican, MISO, NERC, NAGF, PPL, Tampa, UI.

[139] AEP Comments at 6; EEI Comments at 26; Idaho Power Comments at 3-4; NERC Comments at 24; PPL Comments at 6.

[140] KCPL Comments at 4, UI Comments at 7-8.

[141] Luminant Comments at 4; MISO Comments at 6; NERC Comments at 25.

use of a 15-minute parameter to identify generation assets under the CIP version 4 Standards.[142]

120. According to NERC, the 15-minute parameter will typically include SCADA, EMS systems transmission protection systems, and generation control systems. NERC states that the 15-minute parameter will generally exclude systems that collect data for engineering analysis and support, and maintenance, and generally includes systems that provide input to an operator for real-time operations or trigger automated real-time operations.[143] Tampa asserts that Cyber Assets and BES Cyber Systems that actively and directly support the reliable operation of the bulk electric system would be captured under the proposed definition since such assets need to be available at all times.[144]

121. NIPSCO and OEVC contend that the 15-minute parameter is arbitrary and unsupported. NIPSCO states that it is not clear how the 15-minute parameter should be tested or determined under the proposed definition and questions whether responsible entities should be running studies or analysis addressing the loss of cyber assets or whether the 15-minute parameter should be attributed to a cyber asset based on the associated facility.[145] OEVC argues that NERC has not explained the 15-minute

[142] NERC Comments at 24; MISO Comments at 6.

[143] NERC Comments at 26-27. *See also* Tampa Comments at 9.

[144] Tampa Comments at 9.

[145] NIPSCO Comments at 5.

parameter and opines that the 15-minute parameter is "unnecessary as it imposes an arbitrary time period."[146] SPP RE states that it cannot comment on whether the 15-minute parameter is appropriate to establish a distinction between real-time and non-real time operations, but SPP RE is concerned with the audit implications raised by the 15-minute parameter.[147]

Commission Determination

122. We approve NERC's proposed definition of BES Cyber Asset. Based on the comments, we understand that the 15-minute parameter is intended to capture assets involved in real-time operations, such as systems that provide input to an operator for real-time operations or trigger automated real-time operations. According to NERC, "the 15-minute parameter is not about detecting and responding to a Cybersecurity Incident within 15 minutes; rather the 15-minute parameter is about identifying those assets that, when called upon in real-time or rendered unavailable in real-time, could impact reliable operations."[148] The 15-minute parameter is also not without precedent since the

[146] OEVC Comments at 9.

[147] SPP RE Comments at 8-9.

[148] NERC Comments at 26. Further, NERC states that "[t]he 15-minute parameter is essentially used as a measurable proxy for real-time operations in the CIP context," *Id*. at 25. NERC explains that the NERC Glossary defines the term "Real-Time" as "[p]resent time as opposed to future time." The CIP drafting team chose not to use this definition in defining BES Cyber Asset in order to provide a more measurable time frame and avoid confusion during implementation. *Id*.

Commission approved similar language in the CIP version 4 Standards with respect to generating units.[149]

123. As explained by NERC, the 15-minute parameter will typically result in the identification of SCADA, Energy Management Systems, transmission protection systems, and generation control systems as BES Cyber Assets.[150] Further, according to NERC, "[t]ypical systems that might be excluded by the 15-minute parameter are systems that collect data for engineering analysis and support, and maintenance rather than providing input to the operator for real-time operations or triggering automated real-time operations. Such excluded systems would include those used to collect data for the purpose of determining maintenance schedules for assets such as transformers or for engineering analysis."[151] While NERC provides these generalized expectations, NERC also explains that "whether a particular asset is included or excluded from the definition of BES Cyber Asset is necessarily dependent upon the individual facts and circumstances of how an entity uses that asset."[152] We also observe that some commenters express concern over using a time period to determine the impact of a cyber system. Since the identification of BES Cyber Assets is a critical step to applying the CIP version 5

[149] *See* Order No. 761, 139 FERC ¶ 61,058 at P 35 (2012).

[150] *See* NERC Comments at 26.

[151] *Id.*

[152] *Id.* at 27.

Standards, we are interested in better understanding more fully the scope of assets that will be identified as BES Cyber Assets as a result of the application of the 15-minute parameter.

124. Accordingly, the Commission directs NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition. The informational filing should not provide a level of detail that divulges CEII data. This filing should also help other entities implementing CIP version 5 in identifying BES Cyber Assets.

125. The Commission directs NERC to submit the informational filing one year after the effective date of this Final Rule. Based on the information in the informational filing, the Commission may revisit whether the BES Cyber Asset definition should include the 15-minute parameter.

b. 30-Day Exemption

NOPR

126. NERC's proposed definition of BES Cyber Asset 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." In the NOPR, the Commission sought comment on the purpose and anticipated effect of the 30-day exemption language in the BES Cyber Asset definition. Specifically, the Commission sought comment on whether the clause could result in the introduction of malicious code or new attack vectors to an otherwise trusted and protected system, as demonstrated in recent real-world incidents.[153] In addition, the NOPR sought comment on the types of Cyber Assets used for "data transfer, vulnerability assessment, maintenance, or troubleshooting purposes," as this language is used in the BES Cyber Asset definition.[154]

[153] NOPR, 143 FERC ¶ 61,055 at P 78.

[154] *Id.*

Comments

127. Most commenters support the proposed 30-day exemption.[155] NERC and other commenters state that the 30-day exemption is necessary because removing the language would require responsible entities to implement the full set of CIP version 5 requirements on transient systems,[156] which they assert would be impractical and costly.[157] EEI supports the 30-day exemption and maintains that it would be "virtually impossible" for entities to prove compliance with full-time physical security protections around portable devices or programmable electronic devices that are briefly connected to a network and then removed. EEI states that "to practically and auditably preserve the stringent protections in place around BES Cyber Assets as currently defined, the temporarily connected devices…exclusion must be preserved."[158]

128. While some commenters acknowledge that connecting test equipment and other transient systems to trusted networks introduces new attack vectors and potentially malicious code, several commenters, such as MidAmerican, argue that BES Cyber

[155] NERC, EEI, Ameren, AEP, Tacoma, CenterPoint, UI, Dominion, ISO New England, MidAmerican, Exelon, National Grid, NextEra, NorthWestern, PPL Companies, and Wisconsin.

[156] NERC states that "[a]n example of such a transient device is a laptop connected on a temporary basis to run vulnerability assessment software or to perform computer network traffic analysis." NERC Comments at 28.

[157] UI Comments at 8; G&T Cooperatives Comments at 14; NERC Comments at 28.

[158] EEI Comments at 26.

Systems will have adequate security protections by virtue of implementing the CIP version 5 Standards as proposed.[159] Specifically, NERC and others maintain that, since CIP-007-5, Requirement R3 requires the prevention of malicious code, BES Cyber Systems will be safeguarded from threats posed by transient systems.

129. Encari and KCP&L do not support the 30-day exemption in the BES Cyber Asset definition. Encari states that the proposed BES Cyber Asset definition does not adequately address risks posed by transient or temporarily connected systems, adding that the 30-day exemption period appears "arbitrary."[160] Encari also states that this language is prone to abuse, arguing that entities could briefly disconnect Cyber Assets regularly used for used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes in order to restart the 30-day qualification period, making it relatively easy to circumvent CIP implementation on transient systems.

130. KCP&L remarks that "due to a lack of alternative protective measures," it does not support the 30-day language excluding temporarily connected systems.[161] KCP&L believes that implementation of the CIP version 5 standards on transient systems, while burdensome, will prevent a gap in protective measures.[162]

---

[159] CenterPoint Comments at 5; G&T Cooperatives Comments at 14-15; ISO-NE Comments at 11; MidAmerican Comments at 18.

[160] Encari Comments at 4.

[161] KCP&L Comments at 5.

[162] *Id.*

131. Tacoma Power recommends that, since there is no clear guidance as to how transient systems should be managed to ensure malicious code is not introduced into protected environments, clarification is needed.[163]

Commission Determination

132. Based on the explanation provided by NERC and other commenters, we will not direct modifications regarding the 30-day exemption in the definition of BES Cyber Asset. While we are persuaded that it would be unduly burdensome for responsible entities to treat all transient devices as BES Cyber Assets, we remain concerned whether the CIP version 5 Standards provide adequately robust protection from the risks posed by transient devices. Accordingly, as discussed below, we direct NERC to develop either new or modified standards to address the reliability risks posed by connecting transient devices to BES Cyber Assets and Systems.

133. As explained by NERC, the 30-day exemption is intended to remove transient devices from the scope of the CIP version 5 Standards. We recognize that including transient devices in the definition of BES Cyber Asset would subject transient devices to the full suite of cyber security protections in the CIP version 5 Standards. We are persuaded by commenters' explanations 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.

[163] Tacoma Power Comments at 3-4.

134. NERC and other commenters also assert that the CIP version 5 Standards require the protection of BES Cyber Assets from malicious code, thus obviating the need to include transient devices within the scope of the BES Cyber Asset definition. For example, NERC avers that "responsible entities have an affirmative obligation pursuant to CIP-007-5 to prevent malicious code from being introduced on the applicable BES Cyber Systems, no matter where it might originate."[164] However, relying on a single security control to protect information systems is contrary to the fundamental cyber security concept of defense-in-depth, which the Commission continues to believe is the most appropriate way to address cyber security. A transient device introduced directly into a system bypasses most of the protection provided by the layers of security controls provided by the CIP Reliability Standards. It cannot be assumed that anti-malware programs are completely effective in detecting, removing, and blocking malware, especially when they are commonly thwarted by the introduction of zero-day attacks.[165]

135. As the Commission highlighted in the NOPR, transient devices have been the source of incidents where malware was introduced into electric generation industrial control systems in real-world situations.[166] Further, since these devices can move

[164] NERC Comments at 29.

[165] SANS defines a zero-day attack as a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer.

[166] *See* NOPR, 143 FERC ¶ 61,055 at n.69 (referencing Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

(continued…)

between electronic security perimeters, transient devices could spread malware across a responsible entity's BES Cyber Systems absent appropriate controls. While we agree that it would be overly-burdensome to include transient devices in the BES Cyber Asset definition, we agree with Encari and KCP&L that there is a gap in the CIP version 5 Standards regarding transient devices, and these devices pose a risk to BES Cyber Assets that is not addressed in an adequately robust manner in the CIP version 5 Standards.

136. Accordingly, pursuant to section 215(d)(5) of the FPA, the Commission directs NERC to develop either a new or modified Reliability Standard that addresses the risks posed by transient devices. For example, the requirements should recognize that transient devices, unlike BES Cyber Assets, are generally portable and frequently connected and disconnected from systems. The Commission expects NERC to consider the following security elements when designing a Reliability Standard 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). We believe that NIST SP 800-53

Monthly Monitor (October-December 2012) at 1. *Available at* http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_OctDec2012.pdf. The October-December 2012 ICS-CERT Monthly Monitor describes two recent situations where malware was introduced into two electric generation industrial control systems (ICS) through removable media (i.e., USB drive) that was being used to back-up a control system environment and updates.).

Maintenance and Media Protection security control families, as well as the existing Requirements in CIP-004-5, CIP-006-5, and CIP-007-5, can serve as a guide to NERC and the industry in the development of appropriate reliability objectives for transient devices. We believe that addressing transient devices in a new or modified Reliability Standard as discussed above provides a balanced approach to addressing the risks associated with transient devices without imposing unduly burdensome requirements on responsible entities.

2. Definition - Control Center

NERC Petition

137. NERC proposes the following definition of a control center:

> One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

NOPR

138. The Commission sought comment on the meaning of the phrase "generation Facilities at two or more locations" and, specifically, whether the phrase includes two or more units at one generation plant and/or two or more geographically dispersed units.

Comments

139. Commenters generally explain that the phrase "generation Facilities at two or more locations" is intended to capture control centers that control two or more geographically dispersed generation units.[167] NERC and other commenters state that the definition is not intended to capture assets associated with two or more units at one generation plant.[168] Portland opines that an interpretation of the phrase that captures multiple generating units at the same generating plant "could have the unintended consequence of making what are clearly control rooms into control centers."[169]

140. Ameren states that although it understands the term to refer to two or more geographically dispersed units, it would support asking NERC to more clearly define the term.[170] Waterfall advocates for a risk-based definition of control center, noting that the risk control centers pose to the bulk electric system is based on sabotage or mis-operation. According to Waterfall, any set of equipment capable of nearly-

[167] Ameren, Dominion, EEI, Idaho Power, KCP&L, Luminant, MidAmerican, NERC, NAGF, Portland, SPP RE, Tampa, TVA.

[168] Dominion Comments at 14; Idaho Power at 4; MidAmerican Comments at 18; NERC Comments at 30; SPP RE Comments at 10; Tampa Comments at 7.

[169] Portland Comments at 5. *See also* TVA Comments at 6.

[170] Ameren Comments at 17-18.

simultaneously sabotaging a large amount of generating capacity should be classified as a control center no matter where the generation is located.[171]

Commission Determination

141. We approve the definition of Control Center. Consistent with the comments, we clarify that the phrase "generation Facilities at two or more locations" refers to control centers that control two or more geographically dispersed generation units as opposed to assets associated with two or more units at one generation plant. In response to the comments raised by Ameren and Waterfall, we find that definition of Control Center is sufficiently clear. However, entities may seek additional clarification or modification through the NERC standards development process. We also find that the CIP version 5 Reliability Standards take a risk-based approach to Control Centers because, under Reliability Standard CIP-002-5, responsible entities must categorize generation operator Control Centers as High, Medium, or Low Impact based on facility ratings.

3. Definition - Cyber Asset

NERC Petition

142. NERC's currently-effective Glossary definition of Cyber Asset provides:

> Programmable electronic devices and communication networks including hardware, software, and data.

[171] Waterfall Comments at 7.

NERC proposes the following definition of a Cyber Asset:

> Programmable electronic devices, including the hardware, software, and data in those devices.

Thus, NERC's proposed definition of Cyber Asset removes the phrase "communication networks."

NOPR

143. The Commission stated in the NOPR that NERC's proposed definition of Cyber Asset removes the phrase "communication networks" from the currently-effective Glossary definition of Cyber Asset, highlighting the fact that the FPA defines "cybersecurity incident" as follows:

> A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those *programmable electronic devices and communication networks, including hardware, software and data* that are essential to the reliable operation of the bulk power system.[172]

144. The NOPR indicated that NERC's revised definition of Cyber Asset appears to remove a type of asset the statute defines as essential to the reliable operation of the Bulk-Power System.[173]

145. In the NOPR, the Commission sought comment regarding the purpose and intended effect of removing "communication networks" from the definition of a Cyber

[172] NOPR, 143 FERC ¶ 61,055 at P 81 (citing 16 U.S.C. 824o(a)(8) (2012) (emphasis added)).

[173] NOPR, 143 FERC ¶ 61,055 at P 81.

Asset.[174] Further, the Commission sought comment on whether the removal of "communication networks" from the definition could create a gap in cyber security and the CIP Reliability Standards.[175] In addition, the Commission sought an explanation as to the purpose and intended effect of the phrase "data in those devices" and, in particular, whether the phrase excludes data being transferred between devices.[176]

Comments

146. Most commenters support NERC's proposal that removes the phrase "communication networks" from the definition of Cyber Asset.[177] NERC and other commenters contend that the inclusion of communication networks in the currently-effective definition of Cyber Asset has caused confusion in the implementation of the CIP Reliability Standards since communication networks are generally outside the control of responsible entities.[178] NERC, KCP&L, MidAmerican, and Tampa comment that communication networks include programmable electronic device components that could still qualify as Cyber Assets, even though the nonprogrammable electronic

[174] *Id.* P 82.

[175] *Id.*

[176] *Id.*

[177] Ameren, AEP, BPA, Dominion, ISO New England, KCP&L, MidAmerican, MISO, NERC, EEI, Exelon, NAGF, National Grid, NextEra, NorthWestern, Portland, PPL Companies, Tacoma, Tampa, UI, and Wisconsin.

[178] AEP Comments at 6-7; KCP&L Comments at 5; MISO Comments at 7-8; NERC Comments at 31-32; Portland Comments at 5-6.

components of the communication networks, such as cabling, would not qualify.[179] NAGF argues that, although it may be appropriate to address the physical protection of communication cabling in the future, "the remainder of the NERC CIP standards, as currently drafted, cannot be applied to communication cabling."[180]

147. Other commenters claim that removing "communication networks" from the definition of Cyber Asset could create security gaps.[181] SPP RE comments that removing communication networks is inconsistent with the Commission's interpretation of CIP-006-3, Requirement R1.1, which requires the protection of data being transmitted over physical media by either physical or logical means.[182] Idaho Power agrees with the NOPR that excluding communication networks from the Cyber Asset definition could lead to a gap in security; however Idaho Power is concerned about how the CIP version 5 Standards would apply to every component of a communication network.[183] Idaho Power notes that the term "communication network" itself is open to interpretation and creates confusion as to what assets are covered by the CIP Reliability Standards. Therefore, Idaho Power suggests that the Commission direct NERC to define "communication

[179] KCP&L Comments at 5; MidAmerican at 19; NERC Comments at 31-32; Tampa Comments at 8.

[180] NAGF Comments at 6.

[181] Idaho Power, SPP RE.

[182] SPP RE Comments at 11.

[183] Idaho Power Comments at 4.

network" through the standard drafting process and direct NERC to more fully explain how the CIP version 5 Standards would apply to communication networks.[184]

Commission Determination

148. We approve NERC's revised Cyber Asset definition. After considering the explanations provided by commenters, we are persuaded that 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. We further recognize that 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. We anticipate that the removal of this phrase from the Cyber Asset definition will minimize the number of technical feasibility exceptions needed for strict compliance with the CIP version 5 Standards.

149. Nevertheless, we remain concerned that a gap in protection may exist, as the CIP version 5 Standards do not address security controls needed to protect the nonprogrammable components of communications networks. We observe that a number of other information security standards, including NIST SP 800-53 and ISO 27001, address the protection of communication mediums, for instance in NIST SP 800-53 Rev

[184] *Id.* at 5.

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.[185] Similarly, ISO 27001 also emphasizes the protection of telecommunications cabling from interception or damage in control A.9.2.3.[186]

150. We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications 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. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.[187]

---

[185] *See* NIST SP 800-53 Revision 3, security control family Physical and Environmental Protection, Annex 2, page 54.

[186] BSI ISO/IEC (2005). *Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2005).*British Standards Institute

[187] *See infra* P 223.

4. Reliability Tasks

NERC Petition

151. NERC's definitions of the terms BES Cyber System, Control Center, and Reportable Cyber Security Incident include the undefined term "reliability tasks." For example, the proposed definition of BES Cyber System provides:

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

NOPR

152. The Commission raised the concern in the NOPR whether the use of the undefined term "reliability tasks" will lead to confusion during implementation. Therefore, the Commission sought comment on the meaning and scope of the phrase "reliability tasks" and whether there is a common understanding of this phrase to assure accurate and consistent implementation of the definitions and, hence, the CIP version 5 Standards.[188]

Comments

153. Most commenters state that "reliability tasks" has a well-understood meaning and does not need further definition.[189] NERC, EEI, NAGF and other commenters explain that "reliability tasks" refers to the tasks associated with the functions defined in the

[188] NOPR, 143 FERC ¶ 61,055 at P 84.

[189] AEP, CenterPoint, Dominion, EEI, Exelon, Luminant, NERC, NAGF, National Grid, NextEra, NorthWestern, PPL Companies, SPP RE, Tampa, and Wisconsin.

NERC Functional Model.[190] NERC asserts that the use of the undefined term "should not cause confusion in implementation or result in interpretation requests" since industry has a common understanding of the term "reliability tasks."[191] SPP RE and UI explain their understanding of the term "reliability tasks" as referring to the bulk electric system reliability operating services listed in the Guidelines and Technical Basis section of CIP-002-5.[192]

154. Other commenters advocate for defining the phrase "reliability tasks" either because there is no commonly understood meaning or to clarify that the term refers to tasks associated with functions listed in the NERC Functional Model.[193] Ameren suggests that a definition of the term "reliability tasks" reference the CIP-002-5 guidance document to provide more clarity.[194] MISO states that the term "reliability tasks" should be defined in order to avoid ambiguity and to ensure consistent interpretation in enforcement proceedings.[195]

---

[190] AEP Comments at 8; Dominion Comments at 12; EEI Comments at 29; NAGF Comments at 7; NERC Comments at 33-34; Tampa Comments at 8.

[191] NERC Comments at 34.

[192] SPP RE Comments at 11, UI Comments at 10.

[193] Ameren, Idaho Power, KCP&L, and MISO.

[194] Ameren Comments at 18.

[195] MISO Comments at 8.

Commission Determination

155. We are satisfied that responsible entities have a common understanding of "reliability tasks" in the NERC definitions and, thus, we conclude that there is no need to direct NERC to define the phrase. Consistent with the comments of NERC and others, we understand that "reliability tasks" refers to the tasks associated with the functions defined in the NERC Functional Model.

156. While some commenters suggest that the phrase "reliability tasks" is best understood as referring to the bulk electric system reliability operating services listed in the Guidelines and Technical Basis section of CIP-002-5, we believe that the NERC Functional Model is the basis for the phrase "reliability task" while the Guidelines and Technical Basis section provides clarity on how the term applies to the CIP version 5 Standards.

5. Intermediate Devices

NERC Petition

157. NERC proposes to define Electronic Access Control or Monitoring Systems (EACMS) and Interactive Remote Access as follows:

> *EACMS* - Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices.
>
> *Interactive Remote Access* – […] Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). […]

Both proposed definitions include the undefined term "Intermediate Device."

NOPR

158. The Commission explained in the NOPR that the term "Intermediate Systems" was originally referred to as "Intermediate Device" in previous draft versions of the CIP version 5 Standards. The Commission raised the concern that this inconsistency may lead to confusion in the application of the CIP version 5 Standards.[196] Therefore, the NOPR sought comment on whether the defined term "Intermediate Systems" is the appropriate reference in the definitions of Electronic Access Control or Monitoring Systems (EACMS) and Interactive Remote Access, as opposed to the undefined term "intermediate devices."[197]

Comments

159. NERC clarifies that "Intermediate Systems" is the appropriate term in the definitions of EACMS and Interactive Remote Access and states that it will submit an errata change to correct the oversight.[198]

160. In a September 30, 2013 errata filing in this proceeding (docket RM13-5-000), NERC proposes to replace the undefined term "Intermediate Device" with the defined term "Intermediate System" in the definitions of EACMS and Interactive Remote Access.

---

[196] NOPR, 143 FERC ¶ 61,055 at P 85.

[197] *Id.* P 86.

[198] NERC Comments at 35.

Commission Determination

161. The Commission approves the definitions of EACMS and Interactive Remote Access, with the term Intermediate System, as proposed in NERC's September 30, 2013 errata.

D. Implementation Plan

NERC Petition

162. NERC proposes an implementation plan for the CIP version 5 Standards that addresses two distinct issues. First, NERC proposes language that would provide a transition from CIP version 3 to CIP version 5, thereby bypassing implementation of CIP version 4:

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

NERC explains that the language is intended to alleviate uncertainty resulting from "industry stakeholders not knowing whether the Commission will act on CIP Version 5 prior to the CIP Version 4 effective date, April 1, 2014…."[199]

163. Second, NERC proposes a 24-month implementation period for "High Impact" and "Medium Impact" BES Cyber Systems, and a 36-month implementation period for "Low Impact" BES Cyber Systems.

[199] NERC Petition at 43.

NOPR

164. In the NOPR, the Commission proposed to approve the implementation plan for the CIP version 5 Standards to allow responsible entities to transition from compliance with the currently-effective CIP version 3 Standards to compliance with the CIP version 5 Standards, essentially retiring the CIP version 4 Standards prior to mandatory compliance.[200] Thus, upon Commission approval in a Final Rule, the CIP version 5 Standards would supersede Reliability Standards CIP-002-4 through CIP-009-4, and CIP-002-3 through CIP-009-3 would remain in effect and would not be retired until the effective date of the CIP version 5 Standards.

165. With regard to the proposed implementation periods, the Commission sought in the NOPR comment on the activities and any other considerations that justify 24-month and 36-month implementation periods for the CIP version 5 Standards.[201] In addition, the Commission sought comment on whether responsible entities can achieve compliance with the CIP version 5 Standards in a shorter period for those Cyber Assets that responsible entities have identified to comply with the currently-effective CIP Reliability Standards.[202] Finally, the NOPR sought comment on the feasibility of a shorter

[200] NOPR, 143 FERC ¶ 61,055 at P 89.

[201] *Id.* P 90.

[202] *Id.*

implementation period and the reasonable time frame for a shorter implementation period.[203]

Comments

166. While the majority of commenters support NERC's implementation plan as-filed, other commenters either request additional time to implement CIP version 5 or request flexibility to transition to CIP version 5 prior to the proposed effective date.

167. The majority of comments support approval of NERC's implementation plan as-filed.[204] NERC comments that bypassing CIP version 4 will allow entities to devote the necessary resources and attention to implement the improved cyber security controls in CIP version 5. NERC, APPA, CenterPoint, and EEI, among others, identify activities that responsible entities are expected to undertake during the proposed 24- and 36-month implementation periods, including re-evaluating cyber assets and systems based on the new criteria, budget for and acquire resources required to implement the new controls,

[203] *Id.*; *see generally Version 5 Critical Infrastructure Protection Reliability Standards, et al.*, 144 FERC ¶ 61,123 (2013) (granting a six-month extension of the compliance deadline for the CIP version 4 Reliability Standards to facilitate the transition from the CIP version 3 Reliability Standards to the CIP version 5 Reliability Standards).

[204] E.g., Ameren, AEP, APPA, CenterPoint, Consumers Energy, Dominion, EPSA, G&T Cooperatives, Holland, ITC, ISO New England, KCP&L, LADPW, Luminant, MidAmerican, MISO, NASUCA, National Grid, NERC, NAGF, Northeast Utilities, PPL Companies, SCE, SWP, Southern Indiana, Tampa, TVA, UI, and Xcel.

implement the new requirements and then assess implementation of each requirement for compliance.[205]

168. In response to the Commission's concerns about the implementation periods, APPA, Dominion and SWP assert that the 24- and 36-month implementation periods are reasonable, and provide time for entities to budget and acquire the necessary resources to comply with CIP version 5.[206] LADWP cautions that, because vendors of specialized security equipment can require significant lead times and skilled contractors may not be able to implement upgrades within a short period of time, the proposed 24- and 36-month implementation periods are appropriate and necessary.[207]

169. SCE&G contends that the proposed 24-month implementation period for High and Medium Impact assets "is aggressive and likely insufficient."[208] SCE&G proposes that the Commission extend the implementation period for Medium and High Impact assets to 36-months. FirstEnergy supports the proposed implementation plan and notes that the implementation periods "represent an ambitious, but reasonable, industry-vetted goal to

[205] APPA Comments at 19; CenterPoint Comments at 7; EEI Comments at 17-19; LADWP Comments at 15; NRECA Comments at 10; NERC Comments at 37-39; PHI Comments at 2-3; Tampa Comments at 11-12; UI Comments at 3-4.

[206] APPA Comments at 17-19; Dominion Comments at 5-6; SWP Comments at 6.

[207] LADWP Comments at 15.

[208] SCE&G Comments at 6.

achieve compliance with what is essentially a new cyber security framework."[209] Therefore, FirstEnergy asks the Commission to clarify that it will accept, on a case-by-case basis, requests for time extensions to comply with the CIP version 5 Standards when presented with extraordinary circumstances.

170. NRECA and SPP Parties support the proposed 24- and 36-month implementation periods, but suggest that the Commission should permit responsible entities to shift to compliance with the CIP version 5 Standards prior to the effective date.[210] In addition, SPP Parties notes that there is little guidance for entities to transition between the different versions of the CIP Standards and, therefore, entities should not be penalized for maintaining compliance with the prior version of the CIP Standards as they transition to the new version of the standards. Finally, NERC indicates that it plans to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.[211]

Commission Determination

171. The Commission adopts the NOPR proposal to approve the implementation plan for the CIP version 5 Standards as proposed by NERC. Therefore, CIP-002-4 through

[209] FirstEnergy Comments at 4.

[210] NRECA Comments at 10-11, SPP Parties Comments at 4.

[211] *See* NERC Comments at 39-40.

CIP-009-4 will not become effective, and CIP-002-3 through CIP-009-3 will remain in effect until the effective date of the CIP version 5 Standards. In addition, we are persuaded by the majority of commenters that the 24-month implementation period for High and Medium Impact BES Cyber Systems and the 36-month implementation period for Low Impact BES Cyber Systems are reasonable. Commenters cite several potentially resource-intensive tasks, including the hiring and training of new personnel, and activities specific to newly affected BES Cyber Systems, as justification for the 24 and 36-month implementation periods.

172. The Commission also supports NERC's proposal to develop transition guidance documents and a pilot program to assist responsible entities as they move from compliance with the CIP version 3 Standards to the CIP version 5 Standards.[212] The Commission agrees that a pilot program will assist responsible entities by offering best practices and lessons learned during this transition.

173. In response to SCE&G, we decline to extend the proposed 24-month implementation period for Medium and High Impact assets. The overwhelming majority of commenters, including NERC, indicate that the proposed implementation periods are reasonable based on the investments and activities required to implement the CIP version 5 Standards. To the extent that extraordinary circumstances may hinder timely

[212] *See* NERC Comments at 39-40.

compliance, we suggest that responsible entities work with their relevant compliance enforcement authority and NERC to address implementation issues.

174. Similarly, in response to NRECA and SPP Parties, we are not persuaded that there is a need to entertain requests to shift to compliance with the CIP version 5 Standards prior to the effective date of the standards. As NERC notes, the implementation periods and associated pilot program are required, in part, to "allow the Regional Entities and NERC to make adjustments in their systems and approach to compliance with proposed CIP Version 5 while obtaining experience with entities in transition."[213] Issues of early compliance can be addressed by NERC and Regional Entities as appropriate.

E. Violation Risk Factor/Violation Severity Level Assignments

175. NERC requests approval of the Violation Risk Factors (VRF) and Violation Severity Levels (VSL) assigned to the CIP version 5 Standards. In particular, NERC requests approval of 32 VRFs, one set for each requirement in the proposed CIP version 5 Standards.

176. We approve 30 VRFs and direct NERC to modify the VRF for CIP-006-5, Requirement R3 from Lower to Medium and CIP-004-5, Requirement R4 from Lower to Medium. In addition, we direct NERC to modify the VSLs for the CIP version 5 Standards, as discussed below.

[213] NERC Comments at 40.

1. Lower VRF for Maintenance and Testing of Physical Access Control Systems

NERC Petition

177. NERC assigns a Lower VRF to Reliability Standard CIP-006-5, Requirement R3, which addresses the maintenance and testing of Physical Access Control Systems.

NOPR

178. In the NOPR, the Commission stated that the NERC mapping document comparing the CIP version 4 and CIP version 5 Standards identifies Reliability Standard CIP-006-4, Requirement R8, which addresses the maintenance and testing of all physical security mechanisms, as the comparable Requirement in the CIP version 4 Standards.[214] Reliability Standard CIP-006-4, Requirement R8 is assigned a VRF of Medium. The NOPR stated that the Commission's VRF guidelines require, among other things, consistency within a Reliability Standard (guideline 2) and consistency between requirements that have similar reliability objectives (guideline 3).[215] The Commission stated that the petition does not explain the change from a Medium VRF to a Lower VRF for a comparable requirement. The Commission proposed to direct NERC to modify the

[214] Mapping Document Showing Translation of CIP-002-4 to CIP-009-4 into CIP-002-5 to CIP-009-5, CIP-010-1, and CIP-011-1. Page 20-21. Accessible from: http://www.nerc.com/docs/standards/sar/Mapping_Document_012913.pdf.

[215] *See N. Amer. Elec. Reliability Corp.*, 119 FERC ¶ 61,145, *order on reh'g and compliance filing*, 120 FERC ¶ 61,145, at PP 8-13 (2007) (VRF Order). The guidelines are: (1) Consistency with the conclusions of the Blackout Report; (2) Consistency within a Reliability Standard; (3) Consistency among Reliability Standards; (4) Consistency with NERC's Definition of the Violation Risk Factor Level; and (5) Treatment of Requirements that Co-mingle More Than One Obligation.

VRF assigned to CIP-006-5, Requirement R3 from Lower to Medium, consistent with the treatment of the comparable requirement in the CIP version 4 Standards, within 90 days of the effective date of a final rule in this proceeding.

Comments

179. NERC and MISO argue that the Lower VRF for Reliability Standard CIP-006-5, Requirement R3 appropriately reflects the reduced reliability risk in Requirement R3 as compared to CIP-006-4, Requirement R8.[216] NERC states that Requirement R8 requires "[t]esting and maintenance period of all physical security mechanisms on a cycle no longer than three years." NERC states that CIP-006-5 now requires maintenance and testing "at least once every 24 calendar months." NERC asserts that, because maintenance and testing of Physical Access Control Systems will occur more frequently pursuant to the CIP version 5 Standards, the reliability risk is reduced and a Lower VRF is appropriate.

180. Most commenters do not support modifying the VRF proposed by NERC.[217] Commenters state that that the VRF for Requirement R3 should be Lower because Requirement R3 is unlikely to pose a direct threat to reliability if violated. BPA supports the Lower VRF for Requirement R3 because, although "testing and maintenance is an important task, failure to test any single component will have minimal impact of the

[216] NERC Comments at 41-42; MISO Comments at 10.

[217] BPA, Idaho Power, KCP&L, MISO, and NERC.

overall performance of the Physical Access Control System and the BES."[218] However, AEP states that the modification proposed in the NOPR "ensure[s] consistency within a Reliability Standard and consistency between requirements that have similar reliability objectives."[219]

Commission Determination

181. We adopt the NOPR proposal and direct NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium. This modification will ensure that the CIP version 5 Standards afford similar treatment to the testing and monitoring of Physical Access Control Systems (PACS) as the CIP version 4 Standards. We are not persuaded by commenters' arguments that a Lower VRF assignment is appropriate for CIP-006-5, Requirement R3.

182. First, we do not agree that the shortening of the review cycle from three years to two years warrants changing the VRF categorization to Lower as suggested by NERC and MISO. A medium risk requirement is defined as a requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system.[220] Physical Access Control Systems are used to support the effective monitoring and control of the Bulk-

[218] BPA Comment at 9.

[219] AEP Comments at 8.

[220] *See* Violation Risk Factors, accessible from: http://www.nerc.com/files/violation_risk_factors.pdf.

Power System facilities through the use of cameras, alarms, and other control mechanisms. We are not convinced that shortening the required review period from three years to two years ameliorates the potential impact of a violation of this requirement to justify a Lower VRF. A failure to monitor or limit unauthorized access to critical plant equipment or facilities due to an inoperable Physical Access Control System could result in tampering, sabotage, or the unauthorized alteration of equipment associated with High or Medium Impact BES Cyber Systems.

183. In addition, we disagree with BPA's assertion that CIP-006-5, Requirement R3 is administrative in nature and will have a minimal impact on the overall performance of Physical Access Control Systems. As described above, the CIP-006-5, Requirement R3 control is a technical control that sets the minimum expectations for maintenance and testing of Physical Access Control Systems at bulk electric system facilities. Thus, we find that a Medium VRF designation is appropriate for CIP-006-5, Requirement R3.

184. Consistent with our discussion above, the Commission directs NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, within 90 days of the effective date of this Final Rule.

2. Lower VRF for Access Authorizations

NERC Petition

185. NERC assigns a VRF Factor to proposed CIP-004-5, Requirement R4, which relates to access management programs addressing electronic access, unescorted physical access, and access to BES Cyber System Information. Requirement R4 obligates a responsible entity to have a process for authorizing access to BES Cyber System

Information, including periodic verification that users and accounts are authorized and necessary.

NOPR

186. The Commission stated in the NOPR that Recommendation 40 of the U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (Blackout Report) states that access to operationally sensitive computer equipment should be "strictly limited to employees or contractors who utilize said equipment as part of their job responsibilities."[221] In addition, the NOPR stated that Recommendation 44 of the Blackout Report states that entities should "develop procedures to prevent or mitigate inappropriate disclosure of information."[222] The NOPR stated that these two Blackout Report recommendations relate to the protection of critical bulk electric system equipment and information, and we believe these recommendations support assigning access management programs, such as those required under CIP-004-5, Requirement R4, a Medium VRF. The NOPR stated that the Commission's VRF guidelines require, among other things, consistency with the conclusions of the Blackout Report (guideline 1).

[221] *See* U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Blackout Report) at 167. The Blackout Report is *available at* https://reports.energy.gov/BlackoutFinal-Web.pdf.

[222] *See id.* p. 169.

187. The NOPR stated that NERC proposes to assign a Medium VRF to CIP-004-5, Requirement R5, which addresses access revocation. The NOPR stated that this proposed assignment results in a potential inconsistency between VRFs within CIP-004-5. The NOPR stated that Guideline 2 of the Commission's VRF guidelines requires consistency within a Reliability Standard. The NOPR stated that access authorization, addressed in CIP-004-5, Requirement R4, is the companion to access revocation, addressed in CIP-004-5, Requirement R5. The NOPR stated that this relationship is demonstrated by the history of the CIP Reliability Standards; in the CIP version 1 through 4 Standards, access authorization and access revocation are two sub-requirements of a main requirement addressing the maintenance of a list of persons with authorized cyber or authorized unescorted physical access.[223] The NOPR stated that the petition does not explain the potential inconsistency between VRFs in CIP-004-5.

---

[223] *E.g.*, Reliability Standard CIP-004-4a, Requirement R4 states:

> R4. Access —The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
> >
> > R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven

(continued…)

188. The NOPR proposed to modify the VRF assigned to CIP-004-5, Requirement R4 from Lower to Medium, consistent with the Blackout Report and to ensure consistency between VRFs within CIP-004-5, within 90 days of the effective date of a final rule in this proceeding. The NOPR sought comment on the proposal.

Comments

189. NERC states that the Commission should not direct a modification to the VRF for CIP-004-5, Requirement R4. NERC explains that, in developing the VRF for Requirement R4, the drafting team adopted the Lower VRF used in CIP-003-4, Requirement R5, which is the comparable requirement from the CIP version 4 Standards, to provide for consistency. NERC explains further that the standard drafting team concluded that, because Requirement R4 is largely administrative and violations of the requirements do not pose a significant risk to the Bulk Electric System, a Lower VRF was still appropriate. NERC states, by contrast, that the drafting team concluded that a Medium VRF was appropriate for CIP-004-5, Requirement R5 to reflect the greater risk to the bulk electric system in the event of a failure to revoke access. Finally, NERC notes that the standard drafting team determined that failure to revoke access following termination of an employee presents a greater risk to reliability and thus a Medium VRF was appropriate for access revocation.

---

calendar days for personnel who no longer require such access to Critical Cyber Assets.

190. Most comments do not support modifying the VRF proposed by NERC.[224] BPA supports the Lower VRF for CIP-004-5, Requirement R4, because Requirement R4 "concerns only documentation of risk assessment programs and regular performance of background checks."[225] Ameren concurs that CIP-004-5, Requirement R4 is "an administrative documentation requirement [that] does not warrant this heightened level of protection."[226] In addition, Ameren and BPA question the Commission's position that the Blackout Report supports modifying the VRF associated with Requirement R4.[227] Idaho Power opines that a failure to maintain an administrative requirement does not necessarily expose the bulk electric system to a significant risk.[228] MISO, for its part, states that "it is unlikely that violations of [Requirement R4] would pose a direct threat to the reliability of the BES."[229]

191. SPP RE states that it supports the NOPR's proposed modification because "[a]ccess control, both physical and electronic, is a cornerstone to protecting Cyber Assets from unauthorized access. While failure to revoke access is generally considered

[224] Ameren, BPA, Idaho Power, KCP&L, MISO, and NERC.

[225] BPA Comments at 9.

[226] Ameren Comments at 13.

[227] *Id.*

[228] Idaho Power Comments at 7.

[229] MISO Comments at 10.

a greater risk, not properly authorizing access also poses a moderate risk."[230] AEP supports the NOPR's proposed modification to the VRF for Requirement R4 for the same reason that it supports raising the VRF for Reliability Standard CIP-006-5, Requirement R3; specifically, to "ensure consistency within a Reliability Standard and consistency between requirements that have similar reliability objectives."[231]

Commission Determination

192. The Commission adopts the NOPR proposal and directs NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium. This modification is necessary to reflect that access to operationally sensitive computer equipment should be strictly limited to employees or contractors who utilize the equipment in performance of their job responsibilities, and to prevent or mitigate disclosure of sensitive information consistent with Recommendations 40 and 44 of the 2003 Blackout Report. In addition, a Medium VRF assignment ensures consistency with the Commission's VRF guidelines.

193. We disagree with NERC's contention that the risk posed by a violation of CIP-004-5, Requirement R5, which addresses authorization of physical and electronic access, is minor in comparison to a violation of CIP-004-5, Requirement R5, which addresses access revocation. NERC fails to address the concerns raised in the NOPR concerning the inconsistency between the proposed VRF assignments for CIP-004-5, Requirement

[230] SPP RE Comments at 12.

[231] AEP Comments at 8.

R4 and Requirement R5 or explain why we should ignore the Commission's VRF guidelines.

194. We do not agree with NERC, Ameren, and Idaho Power's contention that Requirement R4 warrants a Lower VRF categorization because it is administrative in nature. While CIP-004-5, Requirement R4 mandates that entities must document access and maintain access lists, the underlying control itself is technical in nature because the documented access privileges must be implemented appropriately on the protected devices and in the affected facilities in order to comply with the standard. With respect to Ameren and BPA's comments, the Blackout Report recommendations were intended to address the risks posed by individual grants of access through the use of policies, as the task force specifically recommended that entities develop policies and procedures to control access ensuring that (1) access is strictly limited to employees or contractors who utilize said equipment as part of their job responsibilities and (2) access of other staff are strictly controlled via escort and monitored.[232]

195. We agree with SPP RE that the CIP-004-5, Requirement R4 access authorization process is intended to serve as a preventive control that ensures access is granted on a need to have basis with only the permissions required for job performance. We also agree that the periodic review of access authorizations is a companion detective control

[232] *See* U.S. – Canada Power System Blackout Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations (April 2004) (Blackout Report) at 167. The Blackout Report is *available at* https://reports.energy.gov/BlackoutFinal-Web.pdf.

that is designed to ensure authorized access is still required, and there have been no errors in the granting or revocation of access. When considered in context with the fact that CIP-004-5, Requirement R5 is assigned a Medium VRF, we conclude that a Medium VRF assignment is appropriate for CIP-004-5, Requirement R4.

196. Consistent with the discussion above, we direct NERC to modify the VRF assignment for CIP-004-5, Requirement R4 from Lower to Medium, within 90 days of the effective date of this Final Rule.

3. Violation Severity Levels

NERC Petition

197. NERC requests approval for 32 sets of VSLs – one set for each requirement in the CIP version 5 Standards.[233]

NOPR

198. In the NOPR, the Commission proposed to direct that NERC file a modified version of the VSLs due to inconsistencies with previous Commission orders and typographical errors in the content of the VSLs. The Commission stated that certain VSLs for the CIP version 5 Standards are inconsistent with Commission guidance.[234] The NOPR stated, for example, that Reliability Standard CIP-007-5, Requirement R4.4 requires entities to "review a summation or sampling of logged events … at no greater

[233] NERC Petition at 2.

[234] *N. Amer. Elec. Reliability Corp.*, 123 FERC ¶ 61,284 (Violation Severity Level Order), *order on reh'g*, 125 FERC ¶ 61,212 (2008).

than 15 days." The NOPR stated that the High VSL gradation for Requirement R4.4 provides that an entity must miss "two or more intervals" for the violation to reach High severity over the specified time period. In addition, the NOPR stated that CIP-003-5, Requirement R4 provides the framework for a CIP Senior Manager to delegate authorities and that the proposed VSL is based upon the number of incorrect delegations. The NOPR stated that the Commission has previously indicated that VSL assignments are to be based on "a single violation of a Reliability Standard, and not based on a cumulative number of occasions of the same requirements over a period of time."[235] The NOPR stated that these are two examples of proposed VSL assignments that are inconsistent with the Commission's VSL guidelines.[236]

199. The NOPR stated that certain VSLs are unclear or contain typographical errors. The NOPR stated, as an example, that in the proposed VSL for CIP-004-5, Requirement R4.2, the Moderate and High gradations are identical.[237] The NOPR stated that the

[235] Violation Severity Level Order, 123 FERC ¶ 61,284 at PP 35-36.

[236] The NOPR cited other examples, including the Violation Severity Level assignments for CIP-003-5, Requirement R3, CIP-004-5, Requirement R1, CIP-007-5, Requirement R4, CIP-009-5, Requirement R3.

[237] *See* NERC Petition, Exh. E (Table of VRFs and VSLs Proposed for Approval and Analysis of how VRFs and VSLs Were Determined Using Commission Guidelines), at 21.

typographical errors could create confusion and potentially hinder both compliance with and enforcement of the CIP Reliability Standards.[238]

200. The NOPR stated that NERC also proposes VSLs that include the terms "identify," "assess," "correct," and "deficiencies" for the 16 CIP version 5 "identify, assess, and correct" requirements.[239] The NOPR stated that the Commission may direct modifications to the "identify, assess, and correct" language based on the comments received. The NOPR stated that if the Commission directs NERC to remove or modify the "identify, assess, and correct" language in the requirements, the VSLs may no longer be consistent with VSL Guideline 3, that VSLs use the same terminology as the associated requirement.[240]

201. The NOPR sought comment on the proposal to direct NERC to file a modified version of the VSLs within 90 days of the effective date of a final rule in this proceeding.

---

[238] The NOPR cited the following Requirements: CIP-003-5, Requirements R1, R2, R3; CIP-007-5, Requirement R5; CIP-008-5, Requirements R2, R3; CIP-009-5, Requirements R2, R3.

[239] The NOPR stated that although NERC proposed 17 Requirements with the "identify, assess, and correct" language, the Violation Severity Level assignment for CIP-003-5, Requirement R4 does not refer to the "identify, assess, and correct" language.

[240] *See Automatic Underfrequency Load Shedding and Load Shedding Plans Reliability Standards*, Order No. 763, 139 FERC ¶ 61,098, at PP 91, 95 (2012) (citing VSL Guideline 3, the Commission directed NERC to change a Violation Severity Level for Reliability Standard PRC-006-1, Requirement R8 to remove the phrase "more than 5 calendar days, but" because the Requirement did not contain a five-day grace period for providing data to planning coordinators that was included in the Violation Severity Level).

Comments

202. NERC states that the proposed VSLs are based on a single violation and that "the standard drafting team based its VSL assignment on how much time had passed before the responsible entity complied with the requirement, if ever, not the number of violations."[241] NERC states that it will submit an errata for the VSLs that were unclear or contained typographical errors.[242]

203. BPA supports the VSLs proposed by NERC, stating that "basing the VSL on the number of deficiencies is consistent with the concept of the 'identify, assess, and correct' requirement."[243] Encari supports removing the "identify, assess, and correct" language from the VSLs.

204. Southern Indiana states that it takes no position on the NOPR's proposed modifications to the VSLs. Southern Indiana states that VRFs and VSLs are not dispositive of the level of penalties associated with CIP violations (i.e., there are numerous adjustment factors) and that the Commission should make clear that any penalties for CIP violations should be tailored to each responsible entity's effect on the bulk electric system.

---

[241] NERC Comments at 44.

[242] On September 30, 2013, NERC filed an errata with, *inter alia*, corrections to the VSLs for the CIP version 5 Standards. On October 1, 2013, NERC filed a supplemental errata to correct a formatting error in the September 30 errata.

[243] BPA Comments at 10; KCP&L Comments at 6.

Commission Determination

205. Consistent with the NOPR proposal, we direct NERC to develop modifications to the VSLs for certain CIP version 5 Standard requirements to: (1) remove the "identify, assess, and correct" language from the text of the VSLs for the affected requirements; (2) address typographical errors; and (3) clarify certain unexplained elements. For the VSLs that include "identify, assess, and correct" language, we direct NERC to ensure that these VSLs are modified to reflect any revisions to the requirement language in response to our directives. We grant NERC the discretion to decide how best to address these modifications be it through an errata filing to this proceeding or separate filing.

206. With respect to the VSL language for CIP-003-5, Requirements R1 and R2, the Commission notes that the language "as required by R[1 or 2]" and "according to Requirement R[1 or 2]" is redundant and potentially confusing and hereby directs NERC to provide clarification to this language.

207. With respect to the VSL language for CIP-003-5, Requirement R4, the Commission agrees with NERC that basing the VSL language on a timeline is appropriate, but notes that the VSL language does not match the table and analysis documents within Appendix E of the CIP version 5 Petition. After considering NERC's comments, the Commission understands that the correct VSL for this requirement includes timeline gradations. We therefore direct NERC to clarify the VSL language for this requirement to reflect this understanding.

208. We direct NERC to change the VSL gradation for CIP-004-5, Requirement R4 to be percentage based, instead of using the number of BES Cyber Systems or sites for

storing BES Cyber System information. This change will allow for fair treatment for entities that may only have a single BES Cyber system or storage location.[244]

209. With respect to the VSL language for CIP-008-5, Requirement R2, the Commission believes that NERC inserted a typographical error into the petition, creating a gap between 18 months and 19 months in the VSLs. We therefore direct NERC to clarify this language in a further filing.

210. With respect to the VSL language in CIP-009-5 Part 3.1, we believe that the number of days listed in the VSLs is inconsistent. For example, the moderate VSL for Part 3.1.2 has a timeframe of 90 – 210 calendar days, while the High VSL has a timeframe of greater than 120 calendar days. The Commission believes that the 120 day metric is appropriate for these time-based VSL gradations and directs NERC to change the "210 calendar days" language to "120 calendar days" where appropriate. In short, notwithstanding any changes the Commission requires for VRFs and VSLs, the Commission clarifies that any penalties for violations of the CIP Standards must be tailored to each responsible entity's effect on the BES, with particular consideration given to small utilities that individually pose less of a reliability and security risk.

F. Other Technical Issues

211. In the NOPR, the Commission stated that, "while we propose to approve the CIP version 5 Standards based upon the improvements to the currently-approved CIP

[244] In the September 30 errata, NERC addressed our concern regarding the VSL assignment for CIP-004-5, Requirement R4.

Reliability Standards, we believe that the cyber security protections proposed in the CIP version 5 Standards could be enhanced in certain areas."[245] The NOPR sought comment on the issues of communications security, remote access, and differences between the CIP version 5 Standards and NIST. The Commission further stated in the NOPR that, "depending on the adequacy of the explanations provided in response" to the NOPR questions, the Commission may direct NERC to develop modifications to certain aspects of the CIP Reliability Standards or, alternatively, conclude that while no changes are necessary at this time, NERC must consider these issues in preparing the next version of CIP Standards.[246]

1. Communications Security

NOPR

212. In the NOPR, the Commission stated that communications security, which is a basic layer to any defense-in-depth security strategy for typical industrial control systems, involves securing the data being transmitted across a network. The Commission explained that a variety of cryptographic tools, such as encryption, integrity checks, and multi-factor authentication, can enhance a responsible entity's defense-in-depth security strategies.[247] In addition, the NOPR outlined the Commission's concerns regarding the

[245] NOPR, 143 FERC ¶ 61,055 at P 105.

[246] *Id.*

[247] *Id.* P 107.

exemption of communication networks from protection based solely on specific types of technology, such as non-routable communication systems. The Commission sought comment on (1) whether the adoption of communications security protections, such as cryptography and protections for non-routable protocol, would improve the CIP Standards and (1) whether the CIP standards adequately protect non-routable communication systems.

Comments

213. EEI, MISO, NAGF and other commenters support the concept of communications security through the use of various forms of cryptography as part of a defense-in-depth cyber security posture, although not necessarily as part of the CIP Reliability Standards.[248] NERC, KCP&L, Tacoma and others express concerns regarding potential adverse effects that mandating cryptography for all BES Cyber Systems might have on Bulk-Power System reliability.[249] NERC, EEI, LAWDP and others comment that the deployment of cryptographic protocols may: (1) prohibitively increase latency in communications; (2) obfuscate data needed for testing and problem diagnosis; and (3) introduce communication errors from complex key management across organizations. With regard to the exemption of communication networks, most commenters, including

[248] *See also* Idaho Power; Mid-American; SPP RE; Tampa; Venafi and Waterfall.

[249] *E.g.*, AEP; Idaho Power; PPL and TVA.

NERC, contend that non-routable protocols and devices will be adequately protected under the CIP version 5 Standards.[250]

214. SPP RE, Waterfall, and Venafi comment that protecting communication systems is a critical concept in cyber security and that the use of cryptography under certain circumstances will improve the confidentiality, availability, and integrity of essential data. Thus, they recommend that the Commission require encryption of inter-site communications for communication networks where such protections are readily available and practical.

215. EEI, Dominion, Tacoma Power, TVA, and other commenters indicate that the Commission should refrain from mandating specific technology solutions through mandatory standards, and suggest that cryptography and other emerging technologies should be thoroughly discussed throughout the electric industry. NERC, NAGF, and MISO suggest addressing the NOPR questions on cryptography through a technical conference or other guidance. NERC indicates that a technical conference would provide the appropriate forum to begin discussing the issues associated with communications security and cryptography.

216. With regard to the NOPR concerns regarding the exemption of communication networks from the CIP standards, NERC and other commenters generally agree that additional protections for non-routable protocols and the systems that use them are not

[250] *E.g.*, Dominion; Gist; LADWP; NAGF and Tampa.

needed at this time.[251] NERC explains that the external routable connectivity limitation generally applies to requirements that either require or can take advantage of the high speed connections that are typically associated with routable connectivity. Idaho Power states that non-routable protocols are inherently more secure than routable protocols and states that the CIP Standards provide adequate protection for devices that use non-routable protocols.

2. Remote Access

NOPR

217. "Remote access" refers to the ability to access a non-public computer network from external locations. The Commission explained in the NOPR that, while remote access provides greater flexibility in accessing remote computer networks, this flexibility creates new security risks by allowing a potentially unsecured device access into an entity's network. The Commission discussed the complexities and potential vulnerabilities associated with remote access, including the need for an entity to verify that an employee, vendor automated system initiating remote access to the entity's internal networks has the appropriate access permissions.[252] The Commission requested comment on whether the adoption of more stringent controls for remote access would improve the CIP Reliability Standards.

---

[251] *See,* e.g., Ameren; Dominion; Idaho Power; LADWP; NAGF and TVA.

[252] NOPR, 143 FERC ¶ 61,055 at PP 110-111.

Comments

218. Most commenters assert that the CIP version 5 Standards sufficiently address protections for interactive remote access in CIP-004-5, Requirement R4 and CIP-005-5, Requirement R2.[253] MISO recommends that additional remote access protections beyond those in CIP-005-5, Requirement R2 should be voluntary, due to the differences in entity size and capabilities. EEI and KCP&L assert that remote access issues deserve a thorough discussion and recommendations, not a piecemeal approach.

219. Waterfall comments that remote access mechanisms are among the most serious strategic threats to reliability. Waterfall suggests that, when remote access is needed, unidirectional gateways provide greater security than firewalls and should be mandated by future standards.

3. Differences Between the CIP Version 5 Standards and NIST NOPR

220. In the NOPR, the Commission expressed concern that the CIP version 5 Standards do not address certain aspects of cyber security in as comprehensive a manner as the NIST Risk Management Framework addresses the same topics. The NOPR provided examples of differences between the CIP version 5 Standards and the NIST Risk Management Framework. Such differences include (1) the absence of certain security controls contained in NIST Special Publication 800-53's Security Control Catalog and

[253] *See, e.g.*, Ameren; Dominion; KCP&L; Portland; SPP RE; Tacoma and UI.

associated guidance documents from the CIP version 5 Standards, (2) the failure to address the monitoring of information systems for new threats and vulnerabilities, and (3) comprehensive asset categorization. The Commission sought comment on "whether, and in what way, adoption of certain aspects of the NIST Risk Management Framework could improve the security controls proposed in the CIP version 5 Standards."[254]

Comments

221. NERC states that that the proposed CIP version 5 Standards generally cover the same subject areas as the NIST Risk Management Framework.[255] NERC adds that the question of whether or how to incorporate additional elements of the NIST Risk Management Framework in the CIP Reliability Standards is a discussion for a technical forum inclusive of industry, NERC, and Commission staff.

222. Several commenters discuss the distinctions between the underlying missions of the CIP Reliability Standards and the NIST Risk Management Framework. For example, Waterfall states that the NIST Risk Management Framework, by and large, focuses on securing the confidentiality of data and protecting information systems, not the industrial control systems underlying the reliability of the bulk electric system. Arkansas comments that the CIP Standards have an advantage over the NIST Risk Management Framework in that they focus on a relatively small number of reliability services that

[254] *Id.* P 117.

[255] NERC Comments at 55. *See also* Idaho Power at 9; NAGF at 9-10.

need to be protected as opposed to the NIST mission of establishing general standards for many organizations (all U.S. Federal Agencies) with vastly different missions.

223. Commenters also address differences in the enforcement of the CIP Reliability Standards versus the NIST Risk Management Framework. EEI, ISO-NE, MidAmerican, and Gist state that the NIST Risk Management Framework is a voluntary guidance document that includes control selection, tailoring and scoping of controls to the individual situation, as well as the acceptance of residual risk that FERC has ruled cannot be a part of a mandatory and enforceable Standard. MidAmerican notes further that the CIP version 5 Standards do not allow responsible entities to exercise broad discretion in tailoring their compliance programs and additionally argues that they are generally very prescriptive.

Commission Determination

224. Based on the comments received in response to the NOPR questions, we recognize the broad scope of opinions on the issues of communications security, remote access, and differences between the CIP version 5 Standards and the NIST Risk Management Framework. The NOPR comments indicate a range of views on whether the CIP version 5 Standards adequately address the technical issues discussed in the NOPR, as well as whether and how to address such matters in a future version of the CIP Reliability Standards. Further, we agree with EEI regarding the need to address matters such as remote access, communications security and requiring additional controls in a comprehensive, as opposed to piecemeal, fashion.

225. Accordingly, we decline to direct any modifications to the CIP Reliability Standards at this time to address the NOPR concerns regarding communications security, remote access, and the NIST Risk Management Framework. Rather, we agree with NERC and a number of commenters that suggest a technical conference discussing these issues as an appropriate next step. Accordingly, the Commission directs its staff to convene a staff-led technical conference, within 180 days from the date of this Final Rule, to examine the technical issues identified in the NOPR concerning communications security, remote access, and the NIST Risk Management Framework. While staff should develop a detailed agenda, the conference should address such matters as the adequacy of current coverage in the CIP Standards with regard to the technical issues identified, risks, feasibility, alternative approaches, and a comprehensive approach to addressing defense-in-depth and grid vulnerabilities.

III. Information Collection Statement

226. The FERC-725B information collection requirements contained in this Final Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[256] OMB regulations require approval of certain information collection requirements imposed by agency rules.[257] Upon approval of a collection of information, OMB will assign an OMB control number and

[256] 44 U.S.C. 3507(d) (2012).

[257] 5 CFR 1320.11 (2012).

expiration date. Respondents subject to the filing requirement 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.

NOPR

227. In the NOPR, the Commission estimated a total average annual paperwork cost burden for the change in requirements contained in the CIP version 5 Standards of approximately $56 million. The Commission based its paperwork burden estimate on the difference between the latest Commission-approved version of the CIP Reliability Standards, CIP version 4, and the estimated paperwork burden resulting from CIP version 5 because "the Commission has already imposed the burden of implementing the CIP version 4 Standards" and addressed the incremental burden costs from CIP version 3 to CIP version 4 in the analysis outlined in Order No. 761.[258]

228. In the NOPR, the Commission observed that the change in compliance tasks and paperwork burden between the CIP version 4 Standards and the CIP version 5 Standards varies among entities, depending upon the extent to which an entity was subject to compliance with CIP version 4. Therefore, the Commission delineated three groupings of registered entities for purposes of discussing and refining the burden estimate, and provided separate analysis for each group. To estimate the change in paperwork burden between the CIP version 4 Standards and the CIP version 5 Standards, the Commission

[258] NOPR, 143 FERC ¶ 61,055 at P 119.

identified paperwork-related tasks that all responsible entities will undertake, at least to some extent.[259]

229. In addition, the Commission provided an average annual cost burden for each of the three groups of entities. Referencing Bureau of Labor statistics for the estimated hourly rates and average benefits data, the Commission estimated a total average annual paperwork burden for the change in requirements of $56,112,000.

Comments

230. A number of commenters take issue with the Commission's choice to evaluate the paperwork burden imposed in this Final Rule on an incremental basis from the CIP version 4 Standards to the CIP version 5 Standards, rather than estimate the paperwork burden based on a transition from the CIP version 3 Standards. In addition, various commenters assert that the Commission underestimates the paperwork and cost burdens imposed by the CIP Version 5 Standards.

231. EEI argues that comparing CIP version 5 to CIP version 4 "vastly understates the burden and biases any realistic evaluation," and "strongly disagrees" with this basic assumption of the estimated paperwork burden. EEI contends that a more realistic and practical analysis would compare CIP version 3 and CIP version 5, but admits that such a

[259] Specifically, the Commission determined that responsible entities would be required to, at a minimum: (1) create or modify documentation of processes used to identify and classify the cyber assets to be protected under the CIP Reliability Standards; (2) create or modify policy, process and compliance documentation; and (3) continue documentation of compliance data collection.

comparison would be problematic because the design of the two versions are so different. Therefore, EEI urges the Commission to evaluate the CIP version 5 Standards on their own merits.[260] According to MidAmerican, the Commission's comparison of the two versions, and identification of the burden on responsible entities based on the classes of facilities each group of entities owns, "misses the mark" and, therefore, the Commission grossly underestimated the burden to successfully implement the CIP version 5 Standards.[261] Similarly, NRECA is unclear why the Commission chose to assess the paperwork burden by comparing CIP version 4 and CIP version 5, noting the differences between the two versions and the fact that CIP version 4 will not be implemented. NRECA submits that an appropriate analysis of burden should be based on the full cost of implementing CIP version 5.[262]

232. Tampa states that the level of effort under the CIP version 5 Standards is considerably higher than described in the NOPR due to the volume of new entities and new facilities coming into scope. Tampa points out that entities newly subject to the CIP Reliability Standards "will have a steep learning curve and will need to purchase and

[260] EEI Comments at 24.

[261] MidAmerican Comments at 24-25.

[262] NRECA Comments at 11-12.

install automated workflow and document management systems, which will require time and funding."[263]

233. LADWP states that it expects the impacts of implementing and complying with the CIP version 5 Standards will be substantial, largely resulting from two changes: (1) the elimination of the current blanket exemption for non-routable protocols, and (2) the new requirements in CIP-005-5 that require the expanded use of electronic security perimeters.[264] LADWP estimates that it will make an initial investment of almost $33 million for equipment, materials, and labor. LADWP also estimates that it will spend $3 million annually for software licenses and staff to monitor and implement the CIP version 5 Standards.

Commission Determination

234. For the reasons discussed below, the Commission adopts the Information Collection Statement outlined in the Docket No. RM13-5-000 NOPR.

235. The Paperwork Reduction Act only applies to the paperwork burden imposed by a rule, it does not apply to the substantive requirements imposed by that rule.[265] Commenters generally argue that the Commission underestimates the economic burden of the CIP version 5. However, no commenter provides an analysis regarding the

[263] Tampa Comments at 14-15.

[264] LADWP at 18.

[265] *See* 44 U.S.C. 3506(c)(1) (2012) (outlining the process for the evaluation of a collection of information under a proposed agency rule).

paperwork burden resulting from the approval of the CIP version 5 Standards, as opposed to the anticipated costs of full implementation. For example, NRECA states that its data suggests that the costs associated with the CIP version 5 Standards are an order of magnitude greater than the NOPR estimates. Likewise, LADWP provides a cost estimate for full implantation including equipment, materials and labor, but does not segregate out the paperwork burden relevant to the immediate analysis. Because the Paperwork Reduction Act requires that the Commission estimate the total average annual paperwork cost burden, not the total estimated cost burden of the rule, arguing that the cost of full compliance with CIP version higher than the estimated *paperwork burden* does not negate the Commission's Paperwork Reduction Act estimate.

236. With regard to MidAmerican's and Tampa's comments regarding the costs associated with the expanded scope of the CIP version 5 Standards, we recognize that the CIP version 5 Standards offer a more comprehensive protection of the bulk electric system, particularly due to the coverage of Low Impact assets. Statements regarding the expanded scope of the CIP Reliability Standards alone, without additional data, do not undermine the Commission's approach to estimating the paperwork burden associated with the CIP version 5 Standards or the resulting paperwork burden estimate. The Commission included the cost of developing and modifying the documentation for the required policies, plans, programs and procedures in the paperwork burden estimate, but did not include the cost of substantive compliance with the CIP Reliability Standards. Absent specific comments on the paperwork burden associated with the CIP version 5 Standards, the Commission has no basis to amend the NOPR estimate.

237. In addition, multiple commenters argue that the Commission erred by relying on a burden estimate based on a comparison of the CIP version 5 Standards to the CIP version 4 Standards since the CIP version 4 Standards will not take effect. We reiterate that, in considering and approving the CIP version 4 Standards, the Commission already compared and accounted for the incremental cost burden resulting from the change from the CIP version 3 Standards to the CIP version 4 Standards. Therefore, any incremental change in paperwork burden associated with the approval of the CIP version 5 Standards will be relative to the burden imposed by the approval of the CIP version 4 Standards, whether that change be positive or negative.[266]

238. In reply to concerns regarding potential cost increases associated with changes we direct in this Final Rule, we clarify that any differences in cost will be evaluated at such time as NERC files the directed changes with the Commission.[267]

239. After consideration of comments, the Commission adopts the NOPR proposal for the information collection burden and cost, summarized as follows:

[266] As discussed in the NOPR, we accounted for the provision that CIP version 4 would not go into effect by adjusting the paperwork burden estimate for blackstart facilities – the *only* facilities captured by the CIP-002-4 bright line criteria for full protection, but no longer subject to such protections under the CIP version 5 Standards. *See* NOPR, 143 FERC ¶ 61,055 at PP 123-124.

[267] *See* Order No. 706, 122 FERC ¶ 61,040 at P 800.

Groups of Registered Entities	Classes of Entity's Facilities Requiring CIP Version 5 Protections	Number of Entities	Total Hours in Year 1 (hours)	Total Hours in Year 2 (hours)	Total Hours in Year 3 (hours)
Group A	Low	61	0	3,804	3,804
Group B	Low	1,089	0	570,636	570,636
Group B	Medium	260	128,960	128,960	64,896
Group C	Low	325	0	170,300	170,300
Group C	Medium (New)	78	1,248	1,248	19,136
Group C	Low (Blackstart)	283	22,640	22,640	-206,024
Group C	Medium or High	325	265,200	265,200	135,200
Totals			418,048	1,162,788	757,948

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

- Group A: 61 unique entities * 41.5 hrs/entity * $72/hour = $182,000
- Group B: 1,089 unique entities * 448 hrs/entity * $72/hour = $35,127,000
- Group C: 325 unique entities * 889 hrs/entity * $72/hour = $20,803,000

241. Total average annual paperwork cost for the change in requirements contained in the final rule in RM13-5 = $56,112,000. (i.e., $182,000 + $35,127,000 + $20,803,000).

242. The estimated hourly rate of $72 is the average loaded cost (wage plus benefits) of legal services ($128.00 per hour), technical employees ($58.86 per hour) and administrative support ($30.18 per hour), based on hourly rates and average benefits data from the Bureau of Labor Statistics.[268]

[268] *See* http://bls.gov/oes/current/naics2_22.htm and http://www.bls.gov/news.release/ecec.nr0.htm.

(continued…)

Title: Mandatory Reliability Standards, Critical Infrastructure Protection

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 final rule approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. The approved Reliability Standards help ensure the reliable operation of the Bulk-Power System by providing a cyber security framework for the identification and protection of Critical Assets and associated Critical Cyber Assets. As discussed above, the Commission approves NERC's proposed Version 5 CIP Standards pursuant to section 215(d)(2) of the FPA because they represent an improvement to the currently-approved 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.

243. 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].

244. Comments on the requirements of this rule may be sent 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 RM13-5-000 and OMB Control Number 1902-0248.

IV. Regulatory Flexibility Act Certification

245. The Regulatory Flexibility Act of 1980 (RFA)[269] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. The RFA mandates consideration of regulatory alternatives that accomplish the stated objectives of a proposed rule and that minimize any significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[270] The SBA has established a size standard for electric utilities, stating that a firm is small if, including its affiliates, it is primarily engaged in the transmission,

[269] 5 U.S.C. 601-612.

[270] 13 CFR 121.101 (2012).

generation and/or distribution of electric energy for sale and its total electric output for the preceding twelve months did not exceed four million megawatt hours.[271]

NOPR

246. In the NOPR, the Commission sought comment on the estimated economic impact of implementing and complying with the CIP version 5 Standards. The Commission specifically requested detailed and supported information to better estimate the potential cost burden that small businesses could face under the CIP version 5 Standards.

247. In the NOPR, the Commission estimated that the proposed CIP version 5 Standards, as filed, will impact 536 small entities.[272] The Commission based its estimate of the potential economic impact to small entities according to functional registration and the CIP-002-5 impact rating of assets an entity likely owns by function. Of the 536 total, the Commission estimated that only 14 small entities may, on average, experience a significant economic impact of $116,000 per entity in the first year, $145,000 in the second year, and $88,000 in the third year, for a total of $349,000 per entity over the first three years.[273] The Commission explained that the significant costs in early years are primarily due to initial implementation and, thereafter, the Commission expected the

[271] 13 CFR 121.201, Sector 22, Utilities & n.1.

[272] *See* NOPR at P 132 & n.132.

[273] *See* NOPR, 143 FERC ¶ 61,055 at P 132 (explaining the calculation as based on an estimated 4,600 hours of total work per entity over three years at $59/hour and $15,000 of non-labor costs. (Math correction: $72/hour and $18,000)).

average annual cost per each of the 14 entities to be less than $64,000. The Commission determined that, as 2.6 percent of the affected small entities, these 14 entities do not represent a "substantial number" in terms of the total number of regulated small entities subject to the Final Rule.

248. In addition, the Commission estimated that 222 out of the 536 small entities[274] will each experience an average economic impact of $29,000 per year during years two and three.[275] Finally, the Commission estimated that the remaining 300 out of the 536 small entities will only experience a minimal economic impact.[276] Therefore, the Commission proposed to certify that the proposed Reliability Standards will not have a significant economic impact on a substantial number of small entities, and, accordingly, stated that no initial RFA analysis is required.

Comments

249. Several commenters raise concerns with the Commission's RFA analysis and proposed certification. APPA states that a Final Rule adopting NERC's proposed CIP version 5 Standards as filed will have a "significant economic impact" on all small

[274] *Id*. P 133. The NOPR explained this figure as the number of small entities that own assets covered by CIP version 5, and not including the 14 significantly impacted entities.

[275] The NOPR explained this cost figure as based on an estimated 268 hours of total work per entity for each of years two and three combined at $72/hour, and $7,500 of non-labor costs for each of years two and three.

[276] The NOPR explained this number of small Distribution Providers as those assumed to not own assets covered by CIP version 5.

entities that are registered as transmission owners and transmission operators that own or operate transmission control centers.[277] APPA cautions that it will not condone any Commission RFA certification that denies a "significant impact on a substantial number of small entities."[278] Further, APPA asserts that if the Commission disregards APPA's analysis and adopts the changes proposed in the NOPR, it must conduct a full RFA analysis. [279]

250. APPA contests a number of estimates in the NOPR. APPA states that 327 out of 2,000 not-for-profit publicly owned electric utilities in the United States are on the NERC compliance registry, and approximately 266 of these entities are designated as small entities under the relevant SBA definition.[280] In addition to the 14 small entity transmission owners estimated in the NOPR, APPA identifies 31 small public power transmission operators that it believes are likely to incur significant costs. APPA believes these entities should be added to the 14 identified by the Commission for a total of 45 entities facing a potential significant economic impact.[281] APPA states that the compliance cost burden for High and Medium Impact Control Centers will pose

[277] APPA Comments at 23.

[278] *Id.* at 23.

[279] *Id.* at 30-31.

[280] *Id.* at 24.

[281] *Id.*

particular challenges to small public power entities in economically distressed areas of the United States. On the basis that one of its surveyed members "budgeted $500,000 for developing its CIP compliance program," APPA advocates revising the NOPR estimate upward from $334,000 to $500,000 across the first three years for all 45 entities it believes should be designated as having significant costs.[282]

251. APPA also argues that the NOPR's estimated ongoing economic burden of $64,000 per year is not credible because it is "clearly insufficient to operate and maintain cyber security controls for a bulk electric system-quality control center…and develop and implement an enterprise-wide cyber security program" for Low Impact assets.[283] Based on a range of estimates derived from its survey, APPA arrived at a median annual ongoing cost of $200,000 to maintain security and an additional $50,000 per entity to maintain and carry out the programmatic controls for Low Impact facilities.[284]

252. APPA further identifies 35 discrete small transmission owners that sell less than 1 million megawatt hours a year, stating that "[a]ny increase in compliance costs will be a significant burden to these entities relative to their revenue."[285] APPA states that compliance will force rate increases for these entities that could lead to the loss of key

[282] *Id.* at 28.

[283] *Id.*

[284] *Id.*

[285] *Id.* at 27.

industrial and commercial customers. For each of these entities, and for the remaining entities without High or Medium Impact systems, APPA accepts the Commission estimate of $58,000 for years 1-3, but revises the ongoing cost burden to $50,000.[286]

253. APPA concludes that the total economic burden resulting from the CIP version 5 Standards on all small entities will be $56,349,000.[287] APPA requests that the Commission correct its RFA calculations in the Final Rule and provide more detail on how it arrived at the estimates in the RFA analysis. APPA explains that it requested, but that NERC declined to send out an information request to gather data from small entities on the standard's regulatory impact. APPA requests that, to the extent the Final Rule modifies the CIP version 5 Standards, the Commission direct NERC to provide detailed and supported information regarding the impacts on small entities.[288]

254. NRECA questions the Commission's RFA estimates and requests further explanation of specific assumptions in a manner that would facilitate further comment and analysis. NRECA states that it received estimates from several of its members and concludes that the CIP version 5 Standards, as filed, for entities with only Low Impact assets will cost approximately $100,000 for implementation and then $50,000 annually

[286] *Id.* at 29.

[287] *Id.* at 28.

[288] *Id.* at 31.

thereafter.[289] NRECA states that the Commission provides too little information to support its action of not performing a full regulatory flexibility act analysis.

255. PUCO states that compliance with the CIP version 5 Standards could place heavy financial burdens on smaller utilities, municipalities, and coops. PUCO states further that these entities may not have the same cost-benefit relationship as larger utilities, and that this cost difference should be accounted for in the proposed standards. In addition, PUCO states that investment must be made in a cost effective manner for each utility in a way that protects their high risk vulnerabilities.[290]

Commission Determination

256. Upon consideration of the NOPR comments, we revise our estimate of the number of potentially impacted small entities upwards, from 14 to 45, to reflect the 31 small transmission operators identified by APPA.[291] This number reflects 8.4 percent of the total 536 small entities subject to the CIP version 5 Standards. Further, for the purpose of RFA certification, we will also adopt APPA's cost estimates for the 31 entities added to our analysis, but will maintain our cost estimates for the 14 small entities discussed in the

[289] NRECA Comments at 13.

[290] PUCO Comments at 2-3.

[291] While we question whether available data supports APPA's proposed addition of the 31 small transmission operators discussed above, we will nevertheless adopt APPA's number for the sake of our analysis.

NOPR. Nonetheless, even assuming APPA's cost estimates are correct, we adopt the NOPR proposal and maintain that a full regulatory flexibility analysis is not required.

257. In the NOPR, the Commission estimated that 1.5 percent of the total 305 small entities registered as distribution providers would own underfrequency or undervoltage load shedding systems that were previously not subject to the CIP Reliability Standards, and that 10 percent of the 94 total small entities registered as transmission owners would own Medium Impact assets newly subject to CIP version 5, comprising a total of 14 potentially impacted small entities. The Commission considered the time and expertise needed for an entity to document its asset evaluation process, policy and compliance information, and policy implementation information, as well as install hardware and software, and collect data, to arrive at our estimate of 4,600 hours of total work per entity over three years at an averaged $72 per hour rate for a total $331,000 of labor costs and $18,000 of non-labor costs per entity.

258. In the NOPR, the Commission did not count the small transmission operators identified by APPA because the Commission's analysis assumed that entities had secured the control centers under the CIP version 3 Standards. As noted in Order No. 706, the Commission finds it "difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be identified as a critical asset."[292] We, therefore, accept APPA's

[292] Order No. 706, 122 FERC ¶ 61,040 at P 280.

request to include small entity transmission operators having control centers in our total of small entities significantly affected. We also adopt APPA's suggested figures for costs to secure small transmission operators with control centers, even though APPA provides no detail or support for this figure, as we requested, other than one of its members' planned budgeting for these amounts.

259. We reject APPA's position that 35 small entity transmission owners that sell less than 1 million megawatt hours per year should change our analysis. We understand APPA's argument to rest on the concept that the extra small size of these entities means that they experience the agreed upon compliance cost figure in a proportionately higher manner. Upon evaluating the EIA 2011 data concerning the total revenues for each of the 35 entities listed by APPA, we find that the highest single year cost of $29,000 approaches 0.6 percent of total revenues for only one entity, and is less than 0.3 percent for nearly all of these entities.[293] Viewed across the three-year implementation period, the yearly implementation cost as a percent of total revenues amounts to 0.1 percent when averaged across all 35 entities. Even if these expenses force such an organization into a rate increase, a base of only 2,000 ratepayers would distribute the increase at less than one dollar per month per customer for the three-year period including one year of

[293] *See* Energy Information Administration Form 861 (*available at* http://www.eia.gov/electricity/data/eia861/index.html). The highest year cost of $29,000, as estimated in the NOPR, divided by the total revenue listed in EIA data for a given entity. With the maximum total revenue of $5,021,000, the calculation for Sabine River Authority of TX/LA (Toledo Bend Project) results in 0.58 percent.

on-going costs. For these reasons, APPA has not persuaded us that the 35 extra-small entities will experience proportionately significant costs in the view of the RFA.

260. While APPA asserts that a full RFA analysis is required, we note that we have incorporated relevant portions of APPA's estimates, yet remain unconvinced that the Final Rule will have a significant economic impact on a substantial number of small entities necessitating a more extensive RFA analysis. In addition, we reject the argument that the Commission must revise the NOPR RFA analysis to the extent that the Commission directs modifications to an approved Reliability Standard. We reiterate the Commission's determination in Order No. 706 that until NERC files a revised Reliability Standard, the Commission cannot estimate the burden on any user, owner or operator of the Build-Power System, including small entities, and, therefore, it is not appropriate to speculate on the cost of compliance with any directed modifications at this time.[294]

261. Finally, we reject APPA's request that the Commission direct NERC to provide detailed and supported information regarding the impacts on small entities resulting from any modifications to the CIP version 5 Standards directed in this Final Rule. To the extent that APPA has concerns regarding the cost resulting from a Commission directive, the proper place to raise that concern in the first instance is in the NERC standards development process. In addition, we note that the parties with the best information on the potential impact on small entities resulting from the CIP Reliability Standards are the

[294] *See* Order No. 706, 122 FERC ¶ 61,040 at P 800.

small entities themselves, and we expect such entities to raise their concerns during the standards development process. To the extent that entities provide NERC with such information, we encourage NERC to submit the cost data along with the associated new or revised Reliability Standard requirements.

262. In summary, the Commission estimates that the CIP version 5 Standards will have an economic impact on 536 small entities. The Commission estimates that 14 small entities, registered as transmission owners or distribution providers, and owning a Medium Impact Assets, may experience a significant economic impact of, on average, $116,000 per entity in the first year, $145,000 in the second year, and $88,000 in the third year, for a total of $349,000 over the first three years. After the initial implementation the Commission expects the average annual cost per each of these 14 entities to be less than $64,000. For the sake of this analysis, the Commission expects an additional 31 small entities, registered as transmission operators and operating a Medium Impact control center, to experience a significant economic impact of $518,000 over the first three years and $250,000 ongoing costs per year thereafter. Because we expect the bulk of the initial expense to occur in years two and three, we divide by two to estimate the highest annual cost experienced at $259,000.

263. Together, these two classes of significantly impacted entities comprise 45, or 8.4 percent of the total 536 small entities. The Commission concludes that 8.4 percent of the affected small entities does not represent a substantial number in terms of the total number of regulated small entities, as defined by the RFA, that are subject to the Final Rule. The Commission estimates that 191 out of the 536 small entities will each

experience an average economic impact of $29,000 per year during years two and three, and $13,000 annual ongoing costs thereafter. Finally, the Commission estimates that the remaining 300 out of the 536 small entities will only experience a minimal economic impact. In conclusion, the Commission certifies that this rule will not have a significant economic impact on a substantial number of small entities. Accordingly, a full regulatory flexibility analysis is not required.

V. Environmental Analysis

264. 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.[295] 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 amended.[296] The actions proposed here fall within this categorical exclusion in the Commission's regulations.

[295] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs., Regulations Preambles 1986-1990 ¶ 30,783 (1987).

[296] 18 CFR 380.4(a)(2)(ii).

VI. Document Availability

265. 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.

266. 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 excluding the last three digits of this document in the docket number field.

267. 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 email 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.

VII. Effective Date and Congressional Notification

268. This Final Rule is effective [insert date 60 days from publication in Federal Register].

269. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is a "major rule" as

defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.[297] The Commission will submit the Final Rule to both houses of Congress and to the General Accountability Office.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[297] *See* 5 U.S.C. 804(2) (2007).

Note: the following Appendix will not appear in the *Code of Federal Regulations*.

Appendix
Commenters

Abbreviation	Commenter
AEP	American Electric Power Service Corporation
Alliant	Alliant Energy Corporate Services
Alrich	Tom Alrich
Ameren	Ameren Service Company
APPA	American Public Power Association
Arkansas	Arkansas Electric Cooperative
BPA	Bonneville Power Administration
CenterPoint	CenterPoint Energy Houston Electric, LLC
Consumers Energy	Consumers Energy Company
Dominion	Dominion Resources Services, Inc.
EEI	Edison Electric Institute
Encari	Encari, L.L.C.
EPSA	Electric Power Supply Association
Exelon	Exelon Corporation
FirstEnergy	FirstEnergy Service Company
G&T Cooperatives	Associated Electric Cooperative, Inc., Basin Electric Power Cooperative, and Tri-State Generation and Transmission Association, Inc.
Gist	Thomas Gist
GSOC	Georgia Systems Operations Corp.
Holland	City of Holland, Michigan
Idaho Power	Idaho Power Company
IRC	ISO/RTO Council
ISO New England	ISO New England Inc.
ITC	ITC Companies
KCP&L	Kansas City Power & Light Company and KCP&L Greater Missouri Operations Company
LADWP	City of Los Angeles Department of Water and Power
Luminant	Luminant Generation Company, LLC
MidAmerican	MidAmerican Energy Holdings Co.
MISO	Midcontinent Independent System Operator, Inc.
NAGF	North American Generator Forum
NARUC	National Association of Regulatory Utility Commissioners
NASUCA	National Association of State Utility Consumer Advocates
National Grid	National Grid USA
NERC	North American Electric Reliability Corporation

NextEra	NextEra Energy, Inc.
NIPSCO	Northern Indiana Public Service Co.
Northeast Utilities	Northeast Utilities Companies
NorthWestern	NorthWestern Energy
NRECA	National Rural Electric Cooperative Association
NRG	NRG Companies
OEVC	Occidental Energy Ventures Corp.
Pepco	Pepco Holdings, Inc.
PG&E	Pacific Gas and Electric Company
Portland	Portland General Electric Company
PPL Companies	Louisville Gas and Electric Company; Kentucky Utilities Corporation; Lower Mount Bethel Energy, LLC; PPL Brunner Island, LLC; PPL Electric Utilities Corporation; PPL EnergyPlus, LLC; PPL Holtwood, LLC; PPL Ironwood, LLC; PPL Martins Creek, LLC; PPL Montana, LLC; PPL Montour, LLC; and PPL Susquehanna, LLC.
PUCO	Public Utilities Commission of Ohio
Reclamation	Department of Interior Bureau of Reclamation
SCE	Southern California Edison Company
SCE&G	South Carolina Electric & Gas Company
Southern Indiana	Southern Indiana Gas and Electric Company
Smart Grid	Smart Grid Interoperability Panel Smart Grid Cybersecurity Committee
SPP Parties	Kansas City Board of Public Utilities, Oklahoma Municipal Power Authority, Rayburn Country Electric Cooperative, Southwest Power Pool, Inc., Westar Energy, Inc., and Western Farmers Electric Cooperative
SPP RE	Southwest Power Pool Regional Entity
SWP	California Department of Water Resources State Water Project
Tacoma	Tacoma Power
Tampa	Tampa Electric Company
TAPS	Transmission Access Policy Study Group
TVA	Tennessee Valley Authority
UI	United Illuminating Company
Venafi	Venafi
Waterfall	Waterfall Security Solutions, Ltd.
Wisconsin	Wisconsin Electric Power Company
Xcel	Xcel Energy Services, Inc.