143 FERC ¶ 61,055
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 April 18, 2013)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: Pursuant to section 215 of the Federal Power Act, the Commission proposes to approve the Version 5 Critical Infrastructure Protection Reliability Standards, CIP-002-5 through CIP-011-1, submitted by the North American Electric Reliability Corporation, the Commission-certified Electric Reliability Organization. The proposed Reliability Standards, which pertain to the cyber security of the bulk electric system, represent an improvement over the current Commission-approved CIP Reliability Standards as they adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards. The Commission is concerned, however, that limited aspects of the proposed CIP version 5 Standards are potentially ambiguous and, ultimately, raise questions regarding the enforceability of the standards. Therefore, the Commission proposes to direct that NERC develop certain modifications to the CIP version 5 Standards to address the matters identified by the Commission.

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

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

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

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

FOR FURTHER INFORMATION CONTACT:

Jason Christopher (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) 502-8256

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

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:

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF PROPOSED RULEMAKING

(Issued April 18, 2013)

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission proposes to approve 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 proposed CIP version 5 Standards, which pertain to the cyber security of the bulk electric system, represent an improvement over the current Commission-approved CIP Reliability Standards as they adopt new cyber security controls and extend the scope of the systems that are protected by the CIP Reliability Standards.

2. Specifically, the proposed CIP version 5 Standards include twelve requirements with new cyber security controls. The new controls 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-

[1] 16 U.S.C. 824o (2006).

5), and Configuration Change Management and Vulnerability Assessments (CIP-010-1). As discussed below, the proposed new controls will improve the security posture of responsible entities and represent an improvement in the CIP Reliability Standards.

3. In addition, NERC has proposed to adopt 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. Specifically, NERC has proposed to categorize BES Cyber Systems as having a Low, Medium, or High Impact on the reliable operation of the bulk electric system. Once a BES Cyber System has been categorized, the responsible entity must comply with the associated requirements of the CIP version 5 Standards that pertain to that category. As discussed further below, the proposed approach to categorizing BES Cyber Systems is a step towards applying the CIP protections more comprehensively to better assure the protection of the bulk electric system.

4. While we believe that the proposed CIP version 5 Standards improve the currently-approved CIP Reliability Standards, certain aspects of the proposal raise concerns regarding the potential ambiguity and, ultimately, enforceability of the CIP version 5 Standards. Specifically, seventeen of the requirements of the suite of CIP version 5 Standards include language that requires the responsible entity to implement the requirement in a manner to "identify, assess, and correct" deficiencies.[2] As explained below, we are concerned that this language is unclear with respect to the compliance

[2] *See* NERC Petition at 33.

obligations it places on regulated entities and that it is too vague to audit and enforce compliance. For example, it is unclear whether the inclusion of the "identify, assess and correct" language in the requirements imposes one obligation on the responsible entity (i.e., to ensure the entity has a process in place to identify, assess and correct a violation) 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). Therefore, we seek comment on the meaning of this language and on how it will be implemented and enforced. Depending on the comments and explanations received, we may determine that it is appropriate to direct NERC to develop modifications. For example, the modification may seek to direct NERC to clarify both the compliance obligations created by this language and the criteria by which auditors will be able to determine compliance. Alternatively, we 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. The nature of any next steps will depend on additional information filed with the Commission.

5. In addition, we have concerns with one specific provision, Requirement R2 of Reliability Standard CIP-003-5, which sets forth the single compliance obligation for BES Cyber Systems categorized as Low Impact. Requirement R2 requires responsible entities to "implement … documented cyber security policies that collectively address…" cyber security awareness, physical security controls, electronic access controls and incident response to a cyber security incident. We support extending the scope of the systems that are protected by the CIP Reliability Standards, and believe this is a positive

step forward in comprehensive protection of assets that could potentially cause cyber security risks to the bulk electric system. However, we are concerned that CIP-003-5, Requirement R2 simply requires responsible entities to implement documented policies and does not provide those entities with a clear roadmap of what they need to do in order to protect Low Impact BES Cyber Systems.

6. Beyond the identification of four broad topics, neither this Reliability Standard nor the NERC petition indicate the required content of such policies or the qualitative expectation for an adequate policy. Thus, we are concerned that Requirement R2 is not clear and unambiguous regarding what is required of the responsible entities or, more important, does not provide adequate cyber security controls for Low Impact BES Cyber Assets. Accordingly, as discussed in detail below, we propose to direct that NERC develop modifications to CIP-003-5, Requirement R2, to require that responsible entities adopt specific, technically-supported cyber security controls for Low Impact assets.

7. We also propose to approve the nineteen new or revised definitions associated with the proposed Reliability Standards for inclusion in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). In addition, we seek comment on certain aspects of the proposed definitions. Depending on the comments and explanations received, we may determine that it is appropriate to direct that NERC develop modifications to certain proposed definitions to eliminate ambiguities and assure that BES Cyber Assets are adequately protected.

8. We further propose to approve 30 of the 32 Violation Risk Factors (VRF). However, we propose to direct NERC to modify the VRF assignment for CIP-006-5,

Requirement R3 from Lower to Medium, and to modify the VRF assigned to CIP-004-5, Requirement R4 from Lower to Medium. In addition, we propose to direct NERC to modify the Violation Severity Levels (VSL) for the CIP version 5 Standards. We seek comment on these proposals.

9. We propose 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. Thus, upon approval of the CIP version 5 Standards in a Final Rule in this docket, CIP-002-4 through CIP-009-4 would not become effective, 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. However, we also raise questions 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.

10. The Commission recognizes the ongoing challenge of developing and maintaining meaningful cyber security requirements that set a baseline for protection of the nation's bulk electric system from cyber vulnerabilities. Users, owners and operators of the bulk electric system must adapt to changing threats and cyber technologies to assure the ongoing security of the nation's critical infrastructure. We believe that the modified CIP version 5 Standards proposed by NERC represent an improvement over the previously approved standards and should assist in a more robust cyber security posture for the industry. Therefore, we propose to approve the CIP version 5 Standards. However,

Reliability Standards with unclear requirements or lacking minimum controls can create uncertainty and erode an otherwise effective cyber security posture. Thus, pursuant to section 215(d)(5), we also propose to direct NERC to modify the proposal to remove ambiguous language and assure that Low Impact assets have a clear compliance expectation that includes specified cyber security controls, in lieu of the proposed requirement for unspecified policies, as explained in detail below.

I. Background

A. Section 215 of the FPA

11. Section 215 of the FPA requires the Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and 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.[3] Pursuant to the requirements of FPA section 215, the Commission established a process to select and certify an ERO[4] and, subsequently, certified NERC as the ERO.[5]

[3] *See* 16 U.S.C. 824o(e)(3).

[4] *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).

[5] *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).

B. Order Nos. 706 and 761

Order No. 706

12. 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.[6] 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 the CIP version 1 Standards, intended to enhance the protection provided by the CIP Reliability Standards. Subsequently, NERC filed the CIP version 2 and CIP version 3 Standards in partial compliance with Order No. 706. The Commission approved these standards in September 2009[7] and March 2010,[8] respectively.

Order No. 761

13. On April 19, 2012, the Commission issued Order No. 761, which approved the CIP version 4 Standards (CIP-002-4 through CIP-009-4).[9] Reliability Standard CIP-002-

---

[6] *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).

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

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

[9] *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 FR 24594 (Apr. 25, 2012), 139 FERC ¶ 61,058 (2012) *order denying reh'g*, 140 FERC ¶ 61,109 (2012).

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 to be fully implemented and enforceable beginning April 2014.[10]

II. NERC Petition and Proposed CIP Version 5 Standards

A. NERC Petition

14. In its January 31, 2013 petition, NERC seeks Commission approval of the CIP version 5 Standards, nineteen new or revised Glossary terms, Violation Risk Factors and Violation Severity Levels, and an implementation plan.[11] NERC maintains that the proposed CIP version 5 Standards are just and reasonable, as the proposal meets or exceeds each of the guidelines that the Commission identified in Order No. 672 for evaluating a proposed Reliability Standard.[12] NERC asserts that the proposed CIP version 5 Standards "serve the important reliability goal of providing a cybersecurity

[10] We note that on February 12, 2013, President Barack Obama issued an Executive Order requiring the National Institute of Standards and Technology (NIST) to "lead the development of a framework to reduce cyber risks to critical infrastructure." NIST is required to publish a preliminary version of the framework within 240 days of the Executive Order and a final version one-year after the Executive Order.

[11] Reliability Standards CIP-002-5 through CIP-011-1 are not attached to the notice of proposed rulemaking. 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.

[12] *See* 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)).

framework for the identification and protection of BES Cyber Systems … to support the reliable operation of the Bulk Power System."[13] In addition, NERC states that the proposed CIP version 5 Standards are "designed to be clear and unambiguous" and the Commission should approve the CIP standards as "clearly enforceable."[14]

15. Further, NERC maintains that the proposed CIP version 5 Standards represent a significant improvement to the currently-effective 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.[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."[16] 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."[17]

---

[13] *Id.* at 10.

[14] *Id.* at 27.

[15] *See Id.* at 15.

[16] *Id.*

[17] *Id.*

16. NERC also notes the adoption of new language within several of the CIP version 5 Standards where the Standard Drafting Team incorporated "a requirement that Responsible Entities implement cyber policies in a manner to "identify, assess, and correct" deficiencies."[18] NERC states that the proposed "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*."[19] NERC further states that the "identify, assess, and correct" language "is included as a performance expectation in the requirements, not as an enforcement component."[20]

17. 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."[21] Accordingly, NERC requests that the Commission approve the proposed CIP version 5 Standards, the proposed new and revised definitions, the associated Violation Risk Factors and Violation Severity Levels, and the proposed implementation plan. NERC

[18] *Id.* at 33.

[19] *Id.*

[20] *Id.*

[21] *Id.* at 5.

requests as an effective date for the Reliability Standard, "the first day of the eighth calendar quarter after a Final Rule is issued in this docket."[22]

18. NERC requests prompt Commission action approving the CIP version 5 Standards and associated implementation plan.[23] 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."[24] NERC asserts that prompt approval of the CIP version 5 Standards and implementation plan "would reduce uncertainty among Responsible Entities regarding implementation of the CIP standards."[25]

B. Proposed CIP Version 5 Standards and NERC Explanation of Provisions

19. NERC's proposal includes ten new or modified Reliability Standards.

20. **CIP-002-5 – Cyber Security – BES Cyber System Categorization**: Proposed 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

[22] *Id.* at 2.

[23] *Id.* at 5.

[24] *Id.* at 4.

[25] *Id.* at 5.

Cyber Systems must comply with proposed CIP-003-5 to CIP-011-1, according to specific criteria that characterize the impact of the identified BES Cyber Systems.

21. In particular, proposed 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 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."[26] 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."[27]

22. NERC states that proposed 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.[28]

23. NERC states that proposed CIP-002-5 "Attachment 1 – Impact Rating Criteria" identifies three categories of BES Cyber Systems. The High Impact category covers

[26] *Id.* at 14.

[27] *Id.*

[28] *Id.* at 11.

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 Systems. NERC states that the Low Impact Category provides protections for systems not included in the CIP version 4 Standards.[29]

24. Once a responsible entity identifies a BES Cyber System under CIP-002-5, the entity must comply with the controls included in CIP-003-5 to CIP-011-1 corresponding to its impact category.[30]

25. **CIP-003-5 – Cyber Security – Security Management Controls:** NERC states that proposed 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. Proposed CIP-003-5, Requirement 2, 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.

[29] *Id.*

[30] *Id.*

NERC states that it moved several provisions of requirements related to information protection in previous CIP versions to CIP-011-1 and, therefore, deleted the requirements from CIP-003-5.[31]

26. **CIP-004-5 – Cyber Security – Personnel and Training:** NERC states that proposed 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. Proposed CIP-004-5, Requirement R3, now specifies that the seven year criminal history check covers all locations where the individual has resided for six consecutive months or more without specifying school, work, etc., and regardless of official residence. Proposed 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. Proposed Reliability Standard CIP-004-5 modifies

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

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.[32]

27. **CIP-005-5 – Cyber Security – Electronic Security Perimeter(s):** NERC states that proposed 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 currently-effective CIP-005 Standard 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 CIP version 1 through version 4 was removed from CIP-002-5. Moreover, NERC deleted Requirements R1.1 and R1.3. However, according to NERC, the drafting team integrated the underlying concepts from Requirements R1.1 and R1.3 into the definitions of Electronic Security Perimeter (ESP) and Electronic Access Point (EAP).[33]

28. **CIP-006-5 – Cyber Security – Physical Security of BES Cyber Systems**: NERC states that proposed CIP-006-5 is intended to manage physical access to BES

[32] *Id.* at 12.

[33] *Id.*

Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability. Proposed 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 proposed CIP-006-5.[34]

29. **CIP-007-5 – Cyber Security – Systems Security Management:** NERC states that proposed 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 CIP version 5, along with changes to address several Commission directives and to make the requirements less dependent on specific technology so that they will remain relevant for future, yet-unknown developing technologies. For example, 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.[35]

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

[34] *Id.*

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

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.[36]

31. **CIP-009-5 – Cyber Security – Recovery Plans for BES Cyber Systems:** NERC explains that proposed 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 Systems. Requirement

[36] *Id.* at 13.

R3 establishes a single timeline for a responsible entity to determine the lessons learned and update recovery plans, similar to CIP-008-5.[37]

32. **CIP-010-1 – Cyber Security – Configuration Change Management and Vulnerability Assessments:** NERC states that proposed CIP-010-1 is a new 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.[38]

33. **CIP-011-1 – Cyber Security – Information Protection:** NERC states that proposed CIP-011-1 is a new 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 to BES Cyber System Information. Requirement R2 specifies reuse and disposal provisions to prevent unauthorized dissemination of protected information.[39]

---

[37] *Id.*

[38] *Id.*

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

III. Discussion

34. Pursuant to section 215(d) of the FPA, we propose 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. The proposed CIP version 5 Standards, which pertain to the cyber security of the bulk electric system, represent an improvement over the current Commission-approved CIP Reliability Standards. For example, the CIP version 5 Standards adopt new cyber security controls that are intended to safeguard physical and electronic access to BES Cyber Systems. Further, 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.

35. With regard to controls, the proposed CIP version 5 Standards include twelve requirements with new cyber security controls. These new cyber security controls should improve the defense-in-depth posture of users, owners and operators of the Bulk-Power System. For example, Requirement R1.3 of proposed Reliability Standard CIP-005-5 requires responsible entities to implement inbound and outbound network access permissions, and the reason for granting access. All other access is denied by default. Implementing outbound access permissions can prevent malware from reaching out to a command and control system, potentially reducing the effectiveness of the malware. As another example, pursuant to proposed CIP-005-5, Requirement R1.5, responsible entities must monitor for suspicious inbound and outbound communications at all access points to the Electronic Security Perimeter. Monitoring communications can detect and help prevent malicious code from transferring between networks. Other new controls

pertain to increased minimum protections for remote access (CIP-005-5, Requirement R2), protection against the use of unnecessary physical input/output ports (CIP-007-5, Requirement R1.2), testing recovery plans at least once every 36 months through an operational exercise (CIP-009-5, Requirement R2.3), and developing a baseline configuration of BES Cyber Systems and monitoring for unauthorized changes to the baseline configuration (CIP-010-1, Requirement R1.1 and R2.1). We believe that the proposed new controls will improve the security posture of responsible entities and represent an improvement in the CIP Reliability Standards.

36. In addition, NERC has proposed to adopt 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.[40] Specifically, NERC has proposed to adopt a process that will categorize BES Cyber Systems as having a Low, Medium, or High Impact on the reliable operation of the bulk electric system. Once a responsible entity has categorized its BES Cyber System(s), the responsible entity must then apply the associated requirements of the remaining CIP Reliability Standards, i.e., CIP-003-5 through CIP-011-1. The proposed new approach to categorizing BES Cyber Systems is a step towards applying the CIP protections more comprehensively to better assure the protection of the bulk electric system.

37. Accordingly, for the reasons discussed above, the Commission proposes to approve the CIP version 5 Standards.

[40] *See* Reliability Standard CIP-002-5.

38. We also propose to approve the nineteen new or revised definitions associated with the proposed Reliability Standards for inclusion in the NERC Glossary. In addition, we seek comment on certain aspects of the proposed definitions. Depending on the comments and explanations received, we may determine that it is appropriate to direct that NERC develop modifications to certain proposed definitions to eliminate ambiguities and assure that BES Cyber Assets are adequately protected.

39. We further propose to approve 30 of the 32 Violation Risk Factors (VRF). However, we propose to direct NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, and to modify the VRF assigned to CIP-004-5, Requirement R4 from Lower to Medium. In addition, we propose to direct NERC to modify the Violation Severity Levels (VSL) for the CIP version 5 Standards. We seek comment on these proposals.

40. We propose 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. Thus, upon approval of the CIP version 5 Standards in a Final Rule in this docket, CIP-002-4 through CIP-009-4 would not become effective, 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. However, we also raise questions 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.

41. While we propose to approve the CIP version 5 Standards, we have also identified several concerns with certain provisions of the CIP version 5 Standards. In particular, as discussed in detail below, we are concerned 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 it imposes and that it is too vague to audit and enforce compliance. Therefore, as explained below, we seek comment on this language.

42. Further, the advancement in security resulting from NERC's adoption of a tiered asset categorization, including requiring at least a minimum classification of "Low Impact" for all BES Cyber Systems, can be enhanced by: (1) ensuring that the CIP Reliability Standards are clear, unambiguous, and enforceable; (2) ensuring that the scope of assets covered by the definition of "BES Cyber System" and associated terms captures the right assets for protection; and (3) ensuring that the minimum protections required for "Low Impact" assets are reasonable. Thus, we propose to direct that NERC develop a modification to CIP-003-5, Requirement R2, to require that responsible entities adopt specific, technically-supported cyber security controls for Low Impact assets. We discuss these proposed modifications below.

43. Accordingly, we discuss the following matters below: (A) the "identify, assess, and correct" language; (B) BES Cyber Asset categorization; (C) proposed definitions; (D) implementation plan; (E) Violation Risk Factor and Violation Severity Level assignments; and (F) other technical issues.

A. "Identify, Assess, and Correct" Language

NERC Petition

44. As noted above, 17 requirements of the CIP version 5 Standards incorporate "a requirement that Responsible Entities implement cyber policies in a manner to 'identify, assess, and correct' deficiencies."[41] NERC states that the proposed "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*."[42] During the development of the CIP version 5 Standards, some commenters were concerned that "there is no clear mechanism with how [the proposed "identify, assess, and correct" language] will be audited or that there may be inconsistent audits across Regions."[43] In response, the drafting team stated that the "intent [of the language] is to change the basis of a violation in these requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing and correcting deficiencies."[44]

45. In addition, the drafting team explained that the CIP version 5 Standards are written to require documented processes set forth in the tables that accompany the

[41] Petition at 33.

[42] *Id.*

[43] *Id.* at App. F, Part 2, p. 3435.

[44] *Id.*

requirements. According to the drafting team, in moving toward a risk-based approach, "[e]ntities are to have the processes; the processes must meet the requirements in the tables [of the CIP standards]; and the entities shall implement those processes in a manner that identifies assesses, and corrects deficiencies."[45]

Discussion

46. NERC has not sufficiently explained the proposed "identify, assess, and correct" language, which NERC has elsewhere referred to as "self-correcting language."[46] As we explain below, we are concerned that this language is unclear with respect to the implementation and compliance obligations it places on regulated entities and that it is too vague to audit and enforce compliance. Therefore, we seek comment on the meaning of this language and on how it will be implemented and enforced. Depending on the comments and explanations received, we may determine that it is appropriate to direct NERC to develop modifications. For example, the modification may seek to direct NERC to clarify both the implementation and compliance obligations created by this language and the criteria by which auditors will be able to determine compliance. Alternatively, we may direct NERC to remove this language if it results in requirements

[45] *Id.* at App. F, Part 2, p. 3436.

[46] *See North American Electric Reliability Corporation*, Informational Filing, Docket Nos. RM05-17-000, *et al.*, at 1, n. 3 (filed December 31, 2012) (NERC refers to the "identify, assess, and correct" term as "self correcting language" in the Reliability Standards Development Plan for 2013-2015).

that degrade the protections afforded by the CIP version 5 Standards and are difficult to implement and enforce.

47. Initially, we are concerned that the proposed "identify, assess, and correct" language is unclear with respect to the implementation and compliance obligations it places on regulated entities. For example, it is unclear whether the inclusion of the "identify, assess and correct" language in the requirements imposes one obligation on the responsible entity (i.e., to ensure the entity has a process in place to identify, assess and correct a violation) 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). In the former case, the language could be interpreted or understood to mean that a violation of a Requirement occurs only if the responsible entity did not identify, assess and correct the deficiencies. In the latter case, entities would have to demonstrate that they identify, assess, and correct the deficiencies and, in addition, not violate the underlying requirement.

48. The proposed "identify, assess, and correct" language is ambiguous enough to support both interpretations. Moreover, the comments of the drafting team can be read to support both interpretations. On one hand, the drafting team stated that the "intent [of the language] is to change the basis of a violation in these requirements so that they are not focused on *whether* there is a deficiency, but on identifying, assessing and correcting

deficiencies."[47] This suggests that the language is part of a single compliance obligation and does not impose an additional obligation not to violate the underlying requirement. On the other hand, the drafting team stated that "[e]ntities are to have the processes; the processes must meet the requirements in the tables [of the CIP standards]; *and* the entities shall implement those processes *in a manner* that identifies assesses, and corrects deficiencies."[48] This suggests that the language creates a requirement to "identify, assess and correct" in addition to the obligation to meet the underlying substantive requirement imposed by the standard. Additionally, it is not clear to what extent the drafting team's statement that entities are required to implement processes "*in a manner* that identifies assesses, and corrects deficiencies" permits auditors and the Commission to evaluate the adequacy of an entity's processes or against what criteria they would be evaluated. We seek comment on the purpose of this language and the implications for reliability of both interpretations.

49. Additionally, we are concerned that under either interpretation the proposed the "identify, assess, and correct" language is too vague to be audited. NERC does not explain what is expected of responsible entities or the intended meaning of the individual terms "identify," "assess," "correct," and "deficiencies" as they are used in CIP version 5.

50. As to the term "identify," it is not clear whether a responsible entity is expected to take steps to recognize past deficiencies, ongoing deficiencies, or deficiencies that are

[47] NERC Petition at App. F, Part 2, p. 3435.

[48] *Id.* at App. F, Part 2, p. 3436 [emphasis added].

likely to or may occur in the future. 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. In addition, NERC has not explained what it means for a responsible entity to "correct" a deficiency. 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. NERC does not explain, nor does the text of the CIP version 5 Standards define, the term "deficiencies." It is not clear whether "deficiencies" means "possible violations," as defined in NERC's Compliance Monitoring and Enforcement Program, or extend to a broader category of matters. In short, if a goal of this language is to encourage strong internal controls, the language itself provides no basis for distinguishing strong controls from weak controls and instead leaves this issue to be disputed in future enforcement proceedings. We seek comment on these concerns and on any modification that may be necessary to address them.

51. In addition, the petition does not identify a reasonable timeframe for identifying, assessing and correcting deficiencies. Without identifying a timeframe 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. We seek comment on these concerns and on any modification that may be necessary to address them.

52. The proposed "identify, assess, and correct" language allows a responsible entity to avoid audit risk. Specifically, since there is no 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 petition does not explain whether the responsible entity is required to disclose the identified deficiencies in such cases. Nor is it 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. It is also not clear how prior deficiencies that are identified, assessed and corrected are treated in assessing a responsible entity's compliance history. We seek comment on these concerns and on any modification that may be necessary to address them.

53. The petition does not explain how NERC will treat multiple corrections of deficiencies concerning the same requirement, or the quality of the mitigation. It is unclear whether previous corrections will be reported or otherwise made known to NERC because they are not considered potential violations of the standard. We seek comment on these concerns and on any modification that may be necessary to address them.

54. We are also concerned about how performance of the "identify, assess and correct" phrase can be expected to be uniform or consistent among responsible entities absent additional clarification, explanation or identification of techniques that Regional Entities and NERC would use to determine performance that would comply with requirements that include this phrase. NERC indicates that Audit Worksheets will

address the "identify, assess and correct" provisions. However, the Audit Worksheets have not been developed or submitted for consideration in the petition. We seek comment on these concerns and on any modification that may be necessary to address them.

55. In the petition, NERC states that the "identify, assess, and correct" language is based upon the assess[49] and monitor[50] steps of the NIST Risk Management Framework.[51] NERC does not identify any specific source in these steps of the NIST Risk Management Framework for the "identify, assess, and correct" language. Moreover, both the assess and monitor steps of the NIST Risk Management Framework are tied to guidance publications that establish clear expectations for assessments and continuous monitoring.[52] As noted above, neither the CIP version 5 Standards nor the petition explain what is expected of responsible entities under the proposed "identify, assess, and

[49] SP 800-37 describes the assess step as: "Assess[ing] the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."

[50] SP 800-37 describes the monitor step as: "Monitor[ing] and assess[ing] selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials."

[51] *See* Petition at 32.

[52] *See* SP 800-53A Revision 1, *Guide for Assessing the Security Revision 1 Controls in Federal Information Systems and Organizations* and SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.*

correct" language. We are not opposed to adopting a process to assess and monitor a responsible entity's performance under the CIP Reliability Standards and, in fact, support the idea of having such a process along with clear, well-developed guidance materials. We are concerned, however, that including the assess and monitor processes in the language of a Requirement, as proposed by NERC, could render such provisions unenforceable. We seek comment on these concerns and on any modification that may be necessary to address them.

56. Depending on the comments and explanations received, we may determine that it is appropriate to direct NERC to develop modifications. For example, the modification may clarify the implementation and compliance obligations created by this language, and the standards by which auditors will be able to determine compliance. Alternatively, we 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.

57. We emphasize that our concerns about the proposed "identify, assess, and correct" language should not be read to prejudge the ongoing efforts at NERC to develop changes to the compliance and enforcement program, and this NOPR should not be read as a ruling on that effort. We support wholly NERC's effort to encourage responsible entities to develop internal controls and, moreover, agree that responsible entities should have strong internal controls and receive recognition for such controls when penalties actually are found warranted. Effective internal controls can reduce the need for external enforcement processes, and the resources committed by all participants to these

processes. As the Commission stated in the *Revised Policy Statement on Penalty Guidelines*, "the Penalty Guidelines served only to solidify the importance we place on compliance by providing substantial and transparent mitigation credit for effective compliance programs."[53] We also acknowledge and agree that the resources committed to compliance monitoring and enforcement should be reasonably calibrated to the reliability risks presented.

B. BES Cyber Asset Categorization and Protection

58. Proposed Reliability Standard CIP-002-5 requires responsible entities to categorize BES Cyber Systems as having a Low, Medium, or High Impact. NERC states that proposed 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]."[54] NERC states that the new approach to classifying cyber systems, which requires a minimum classification of "Low Impact" for all BES Cyber Systems, "resulted from a review of the NIST Risk Management Framework for

[53] *Revised Policy Statement on Penalty Guidelines*, 132 FERC ¶ 61,216, at P 109 (2010).

[54] Petition at 11.

categorizing and applying security controls, a review that was directed by the Commission in Order No. 706."[55]

59. NERC's new approach to categorizing BES Cyber Systems is a step closer to comprehensively protecting assets that could cause cyber security risks to the bulk electric system. However, as discussed below, the Commission believes that NERC should consider improving the categorization process and should modify the minimum protections required for "Low Impact" assets to identify specific controls.

1. Reliability Based Criteria

60. In Order No. 706, the Commission directed NERC to "monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards."[56] The incorporation of new NIST-like concepts into the CIP Reliability Standards, such as the Low-Medium-High categorization, is encouraging. However, as discussed below, significant differences exist between the NIST Risk Management Framework and the proposed CIP version 5 Standards, particularly with regard to system identification and categorization.

61. As noted above, proposed Reliability Standard CIP-002-5 requires each responsible entity to categorize BES Cyber Systems as having a Low, Medium, or High Impact based on the adverse impact that loss, compromise, or misuse of its BES Cyber

[55] *Id.* at 15.

[56] Order No. 706, 122 FERC ¶ 61,040 at P 233.

Systems could have on the reliable operation of the bulk electric system. NERC states that this categorization process is based upon the NIST Risk Management Framework. The NIST Risk Management Framework, however, utilizes a categorization process based on the loss of confidentiality, integrity, and availability of systems, as defined in the Federal Information and Security Act of 2002.[57]

62. The NIST Risk Management Framework requires a low, moderate, or high level of protection for devices, systems, and associated data based on the criticality of the protected information.[58] The categorization process establishes a foundation for security standardization across different types of data, controls, and equipment.[59] While the CIP version 5 Standards share a similar grouping of Low-Medium-High categories with the

[57] *See Federal Information and Security Act of 2002*, 44 U.S.C. 3542 (2002) (Confidentiality is defined as preserving authorized restrictions on access and disclosure, including a means for protecting personal privacy and proprietary information; integrity as guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; availability as ensuring timely and reliable access to and use of information).

[58] *See* NIST Special Publication 800-60, at 9. According to NIST, "security categories are based on the potential impact on an organization should certain events occur. The potential impacts could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."

[59] *See* NIST Special Publication 800-60 at 4-5. NIST states that the value of information security categorization is to enable organizations "to proactively implement appropriate information security controls based on the assessed potential impact to information confidentiality, integrity, and availability and in turn to support their mission in a cost-effective manner."

NIST Risk Management Framework, the categorization processes proposed under the CIP version 5 Standards and the NIST Risk Management Framework are different. Rather than categorize assets based on the loss of confidentiality, integrity, and availability of systems, CIP-002-5 categorizes assets based on "reliability impact."

63. Specifically, the reliability impacts underlying the CIP-002-5 asset categorizations are based on facility ratings, such as generation capacity and voltage levels. For example, the CIP-002-5 – Attachment 1 Impact Rating Criteria establishes a threshold for "Medium Impact" generation at 1500 MW. This determination is based on the assumption that generation facilities with smaller values would have a "Low Impact" on grid reliability.[60] However, the petition does not contain or reference reliability studies that provide the supporting engineering analysis for such thresholds. For example, the "Medium Impact" thresholds for both generation and transmission do not seem to consider the impacts of a coordinated attack on "Low Impact" systems, such as the loss of several or all 100 kV facilities owned or operated by a single entity.

64. NERC's proposed categorization process is based on facility ratings, such as generation capacity and voltage levels. As discussed elsewhere, the NIST Risk Management Framework categorizes systems based on cyber security principles regarding the confidentiality, integrity, and availability of systems.[61] We accept NERC's

[60] *See* Reliability Standard CIP-002-5 - BES Cyber System Categorization, at Attachment 1.

[61] For example, the ISA99 suite of standards (also known as ISA/IEC-62443:

(continued…)

proposal at this time. However, we may revisit the categorization of assets under the CIP Reliability Standards at a later date.

2. Protection of Low Impact BES Cyber Assets

65. 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.

"Security for Industrial Automation and Control Systems") utilizes an approach similar to what is outlined in the NIST Framework and further clarifies system impact to mean "impacts that might result from security failures, taking into account the consequences of a loss of confidentiality, system integrity, or availability of the assets, loss of reliability and manipulation of the [industrial control system]." See ISA/IEC-62443-2-1, 2013 Draft. Requirement 4.4.2.1. Establishing and Managing the Industrial Automated Control System Security Management System. http://isa99.isa.org/Documents/Drafts/ISA-d62443-2-1.pdf

66. NERC states that the proposed CIP version 5 Standards require a minimum classification of "Low Impact" for all BES Cyber Systems that are not classified as either "Medium" or "High" Impact. The proposed new approach to identify Low Impact BES Cyber Systems is a positive step towards applying the CIP Reliability Standards in a more comprehensive manner to better assure the protection of the bulk electric system. However, we have concerns regarding Requirement R2 of Reliability Standard CIP-003-5, which sets forth the single compliance obligation for BES Cyber Systems categorized as Low Impact. Requirement R2 requires responsible entities to "implement … documented cyber security policies that collectively address…" cyber security awareness, physical security controls, electronic access controls and incident response to a cyber security incident. Further, CIP-003-5, Requirement R2, simply requires responsible entities to implement documented policies, which could allow insufficient protection to Low Impact BES Cyber Assets.

67. Under the proposed CIP version 5 Standards, a responsible entity is required to document and implement both policies and procedures to perform the specific requirements of CIP-003-5 through CIP-011-1 for systems identified as High or Medium Impact pursuant to the criteria in proposed CIP-002-5.[62] By contrast, a responsible entity is only required to have "documented cyber security policies" for Low Impact BES

[62] *See* Reliability Standard CIP-003-5 - Cyber Security – Security Management Controls, at Requirement R1.

Cyber Systems; there is no requirement to implement actual cyber security protections.[63] While the Commission believes that an individual Medium or High Impact asset will have higher potential reliability impacts as compared to an individual Low Impact asset, the Reliability Standards must also enumerate specific, technically-supported cyber security controls for Low Impact assets.

68. We support NERC's efforts to increase the scope of systems that are protected by the CIP Reliability Standards, but the lack of specificity regarding the content of the four policies covering Low Impact BES Cyber Systems raises the prospect of an ambiguous Reliability Standard that will be difficult for responsible entities to implement.

69. Our concern is highlighted by NERC's supporting materials for proposed Reliability Standard CIP-003-5. For example, while Requirement R2.3 requires responsible entities to have policies on electronic access controls, the Guidelines and Technical Basis for CIP-003-5 pertaining to Requirement R2.3 states that "electronic access control" is not meant "in the specific technical sense requiring authentication, authorization, and auditing."[64] However, it is unclear how an entity can perform electronic access control without some form of authentication or authorization. We also question whether the proposal to require a policy document can be considered

[63] *See* Reliability Standard CIP-003-5 - Cyber Security – Security Management Controls, at Requirement R2.

[64] *See* Reliability Standard CIP-003-5 - Cyber Security – Security Management Controls, at Page 18.

implementing "electronic perimeter protection," which NERC states is required at every impact level to implement a "mutual distrust" posture across all BES Cyber Systems.[65]

70. We are concerned 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, results in ambiguity that may 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. Therefore, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to 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. We seek comment on this proposal. In particular, we seek comment on the value of adopting specific controls for Low Impact assets that reflect their cyber security risk level, similar to the NIST Risk Management Framework.

71. Also, we seek comment on the lack of a requirement to have an inventory, list or discrete identification of Low Impact BES Cyber Systems. The definition of BES Cyber Systems is a threshold for determining applicability of the CIP Reliability Standards, so we assume responsible entities will in fact start by identifying all covered systems. If so, the rationale or benefit for not requiring an inventory, list or identification is unclear.

[65] *See* Petition at 40.

C. Proposed Definitions

72. The proposed CIP version 5 Standards include nineteen definitions for inclusion in the NERC Glossary. This includes the addition of fifteen new definitions and four revised definitions, as well as the retirement of two definitions.[66] We propose to approve the proposed definitions for inclusion in the NERC Glossary.

73. We also seek comment on certain aspects of the proposed definitions. After receiving comments, depending on the adequacy of the explanations provided in response to our questions, we may direct NERC to develop modifications to certain proposed definitions to eliminate ambiguities and assure that BES Cyber Assets are adequately protected.

Definition - BES Cyber Asset

74. In its Petition, 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

[66] 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.

> 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.)

75. The first step in determining whether the substantive requirements of the CIP Reliability Standards apply is the identification of BES Cyber Assets pursuant to CIP-002-5. If an entity does not identify a BES Cyber Asset, the remaining CIP Reliability Standards do not apply. Thus, a clear understanding of the definition of BES Cyber Asset is important to assure accurate and consistent application of the CIP version 5 Standards.

76. The definition begins with "[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…." The CIP version 4 Standards include a 15 minute parameter for the identification of Critical Cyber Assets associated with generation units at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection.[67] The drafting team adopted the 15 minute parameter in CIP version 4 in recognition of a concern that "there may be Facilities which, while essential to the reliability and operability of the generation facility, may not

[67] *See* Reliability Standard CIP-002-4a (Critical Cyber Asset Identification), at Requirement R2.

have real-time operational impact within the specified real-time operations impact window of 15 minutes."[68] An example considered during the development of CIP version 4 was a coal-handling facility, the outage of which typically does not disrupt operations until after at least a short period of time. Thus, the 15 minute language found in the CIP version 4 Standards is tailored to address a specific concern with one class of assets. NERC now proposes to adopt similar 15 minute language in relation to all Cyber Assets associated with all classes of assets without explanation.

77. We seek comment on the purpose and effect of the 15 minute limitation. In particular, we seek comment on the types of Cyber Assets that would meet the "within 15 minutes" caveat. Further, we seek comment on the types of assets or devices that the 15 minute language would exclude and, in particular, whether the caveat "within 15 minutes" exempts devices that have an impact on the reliable operation of the bulk electric system. We also seek 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.

78. The proposed definition of BES Cyber Asset also provides 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

[68] NERC Petition, Docket No. RM11-11-000, at 16 (filed Feb. 10, 2011)

an [Electronic Security Perimeter], or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes." We seek comment on the purpose and anticipated effect of this provision in identifying BES Cyber Assets. Specifically, we seek 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.[69] In addition, we seek comment on the types of Cyber Assets used for "data transfer, vulnerability assessment, maintenance, or troubleshooting purposes," as this language is used in the proposed BES Cyber Asset definition. If the terms cited here leave unreasonable gaps in the applicability of the CIP Reliability Standards, we will direct appropriate modifications.

Definition - Control Center

79. 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.

[69] *See* Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Monthly Monitor (October-December 2012) at 1. Available at http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.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 update software.

80. We seek 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.

Definition - Cyber Asset

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

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

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." We note 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.[70]

Thus, it appears that NERC's revised definition of Cyber Asset removes a type of asset the statute defines as essential to the reliable operation of the Bulk-Power System.

82. We seek from NERC and other commenters an explanation for the purpose and intended effect of removing "communication networks" from the definition of a Cyber Asset. Further, we seek comment whether the removal of "communication networks" from the definition could create a gap in cyber security and the CIP Reliability Standards.

---

[70] 16 U.S.C. 824o(a)(8) (2006) (emphasis added).

In addition, we seek comment on the purpose and intended effect of the phrase "data in those devices" and, in particular, whether the phrase excludes data being transferred between devices.

Reliability Tasks

83. The term "reliability tasks" is an undefined term used in NERC's proposed definitions of BES Cyber System, Control Center, and Reportable Cyber Security Incident. 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.

84. We are concerned that the use of the undefined term "reliability tasks" will likely lead to confusion during implementation and result in interpretation requests. We seek 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.[71]

Intermediate Devices

85. 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

[71] We note that the term "reliability tasks" is used in the NERC Functional Model to register entities based upon their responsibilities for the reliable operation of the Bulk-Power System.

> 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 devices." The proposed defined term "Intermediate Systems" was originally referred to as "Intermediate Device" in previous draft versions of the CIP version 5 Standards.[72] This inconsistency may lead to confusion in application of the CIP version 5 Standards.

86. Therefore, we seek comment on whether the proposed defined term "Intermediate Systems" is the appropriate reference in the proposed definitions of Electronic Access Control or Monitoring Systems (EACMS) and Interactive Remote Access, as opposed to the undefined term "intermediate devices."

D. Implementation Plan

87. NERC's proposed implementation plan for the CIP version 5 Standards 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. Specifically, the proposed language provides:

> Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through

[72] The first balloted draft of the proposed CIP version 5 Standards included a definition for "Intermediate Device." The name of this term did not change to "Intermediate System" until the fourth and final balloted draft.

> 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 states that the proposed 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…."[73]

88. 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. The NERC petition does not provide an explanation or justification for the proposed implementation periods.

89. We propose 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. Thus, upon approval of the CIP version 5 Standards in a Final Rule in this docket, CIP-002-4 through CIP-009-4 would not become effective, 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. However, we do not see why the 24-month and 36-month implementation periods proposed by NERC for the CIP version 5 Standards are necessary.

90. We seek comment on the activities and any other considerations that justify 24-month and 36-month implementation periods for the CIP version 5 Standards. We seek

[73] Petition at 43.

an explanation of the activities that responsible entities will have to undertake to achieve timely compliance with the CIP version 5 Standards. We also seek 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. Finally, we seek comment on the feasibility of a shorter implementation period and the reasonable time frame for a shorter implementation period. If the comments do not provide reasonable justification for the proposed implementation periods, we will direct appropriate modifications.

E. Violation Risk Factor/Violation Severity Level Assignments

91. 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. As explained below, we seek comment on our proposal to accept 30 VRFs and to direct NERC to develop modifications to two VRFs. Specifically, we seek comment on our proposal to direct NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, and to modify the VRF assigned to CIP-004-5, Requirement R4 from Lower to Medium. In addition, we propose to direct NERC to modify the VSLs for the CIP version 5 Standards.

Lower VRF for Maintenance and Testing of Physical Access Control Systems

92. NERC assigns a Lower VRF to proposed CIP-006-5, Requirement R3, which addresses the maintenance and testing of Physical Access Control Systems (PACS). The NERC mapping document comparing the CIP version 4 and CIP version 5 Standards

identifies 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.[74] Reliability Standard CIP-006-4, Requirement R8 is assigned a VRF of Medium.

93. Our Violation Risk Factor guidelines require, among other things, consistency within a Reliability Standard (guideline 2) and consistency between requirements that have similar reliability objectives (guideline 3).[75] The petition does not explain the change from a Medium VRF to a Lower VRF for a comparable requirement. We propose to modify the VRF assigned to CIP-006-5, Requirement R3 from Lower to Medium. However, NERC and other commenters are free to provide additional explanation than provided thus far to demonstrate CIP-006-5, Requirement R3 is properly assigned a Lower VRF.

94. On this basis, we seek comment on our proposal to direct NERC to modify the VRF assignment for CIP-006-5, Requirement R3 from Lower to Medium, consistent with

[74] 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

[75] *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.

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.

Lower VRF for Access Authorizations

95. NERC assigns a Lower VRF 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.

96. 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."[76] In addition, Recommendation 44 of the Blackout Report states that entities should "develop procedures to prevent or mitigate inappropriate disclosure of information."[77] These two Blackout Report recommendations relate to the protection of critical bulk electric system equipment and

[76] *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.

[77] *See Id.* p 169.

information, and we believe these recommendations support assigning access management programs, such as those required under CIP-004-5, Requirement R4, a Medium VRF. Our Violation Risk Factor guidelines require, among other things, consistency with the conclusions of the Blackout Report (guideline 1).

97. In addition, NERC proposes to assign a Medium VRF to CIP-004-5, Requirement R5, which addresses access revocation. This proposed assignment results in a potential inconsistency between VRFs within CIP-004-5. As noted above, Guideline 2 of our Violation Risk Factor guidelines requires consistency within a Reliability Standard. Access authorization, addressed in CIP-004-5, Requirement R4, is the companion to access revocation, addressed in CIP-004-5, Requirement R5. 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.[78] The petition does not explain the potential inconsistency between VRFs in CIP-004-5.

---

[78] *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.

(continued…)

98. We propose to modify the VRF assigned to CIP-004-5, Requirement R4 from Lower to Medium. However, NERC and other commenters are free to provide additional explanation than provided thus far to demonstrate CIP-004-5, Requirement R4 is properly assigned a Lower VRF.

99. We seek comment on our proposal to direct NERC to change the VRF assignment for 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.

Violation Severity Levels

100. NERC requests approval for 32 sets of VSLs – one set for each requirement in the CIP version 5 Standards.[79] Due to inconsistencies with previous Commission orders and various typographical errors in the content of the VSLs, we propose to direct NERC to file a modified version as discussed below.

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

[79] Petition at 2.

101. Certain VSLs for the CIP version 5 Standards are inconsistent with previous Commission guidance.[80] For example, proposed CIP-007-5, Requirement R4.4 requires entities to "review a summation or sampling of logged events … at no greater than 15 days." The High VSL gradation for Requirement R4.4 states that an entity must miss "two or more intervals" for the violation to reach High severity over the specified time period. In addition, CIP-003-5, Requirement R4 provides the framework for a CIP Senior Manager to delegate authorities. The proposed VSL is based upon the number of incorrect delegations. The Commission has previously stated 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."[81] These are two examples of proposed VSL assignments that are inconsistent with the Commission's VSL guidelines.[82]

102. Also, certain VSLs are unclear or contain typographical errors. For instance, the proposed VSLs for CIP-004-5, Requirement R4.2's Moderate and High gradations are

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

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

[82] Further examples of this concern include VSL assignments for the following: CIP-003-5, Requirement R3, CIP-004-5, Requirement R1, CIP-007-5, Requirement R4, CIP-009-5, Requirement R3.

identical.[83] Such typographical errors will create confusion and potentially hinder both compliance with and enforcement of the CIP Reliability Standards.[84]

103. NERC also proposes VSLs that include the terms "identify," "assess," "correct," and "deficiencies" for the 16 CIP version 5 "identify, assess and correct" Requirements.[85] As noted above, we seek comment on these terms and may direct modifications based on the comments received. If we do so, the VSLs may no longer be consistent with VSL Guideline 3, that VSLs use the same terminology as the associated requirement.[86]

104. Therefore, for the reasons outlined above, we seek comment on our 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.

---

[83] *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.

[84] The Requirements that raise this concern include: CIP-003-5, Requirements R1, R2, R3; CIP-007-5, Requirement R5; CIP-008-5, Requirements R2, R3; CIP-009-5, Requirements R2, R3.

[85] Although NERC has proposed 17 requirements with the "identify, assess, and correct" language, the VSL assignment for CIP-003-5, Requirement R4 does not refer to the "identify, assess, and correct" language.

[86] *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 VSL 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 VSL).

F. Other Technical Issues

105. While we propose to approve the CIP version 5 Standards based upon the improvements to the currently-approved CIP Reliability Standards discussed above, we believe that the cyber security protections proposed in the CIP version 5 Standards could be enhanced in certain areas. Therefore, we invite comment on the issues outlined below. After receiving comments, depending on the adequacy of the explanations provided in response to our questions, we may direct NERC to develop modifications to certain aspects of the CIP Reliability Standards to assure that BES Cyber Assets are adequately protected. Alternatively, we may conclude that while no changes are necessary at this time, NERC must consider these issues in preparing the next version of CIP Standards.

1. Communications Security

106. Protecting communications systems is a critical concept in cyber security. Communications security involves securing the data being transmitted across a network.[87] Secure data transmission is a basic layer to any defense-in-depth security strategy for typical industrial control systems.[88] When addressing cyber security for

[87] *See* NIST Interagency Report 7298, *Glossary of Key Information Security Terms*, which defines communication security (COMSEC) as a "component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material."

[88] *See* NIST Special Publication 800-82, *Guide to Industrial Control Systems Security*, at page 3. According to NIST, "in a typical ICS…a defense-in-depth strategy… includes… applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate."

electric power systems, communications security should protect and ensure the confidentiality, integrity, and availability of the data and functions used to support the reliable operation of the Bulk-Power System.

107. We believe that the adoption of cryptography would improve the approach adopted in the CIP version 5 Standards.[89] Cryptography is a branch of mathematics that provides communications protection.[90] Cryptography is a useful technique to protect data that is utilized for both smart grid applications[91] and in other industries,[92] including the natural gas[93] and nuclear power industries.[94] Cryptography ensures the confidentiality of sensitive information, ensures the integrity of data and commands, determines if data has been modified, and authenticates the identity of the sender. A

[89] The CIP version 5 Standards address the use of cryptography in only one instance, regarding interactive remote access. *See* Reliability Standard CIP-005-5 - Cyber Security – Electronic Security Perimeters, Requirement R2.2, at Page 16.

[90] *See* NIST Special Publication 800-21. According to NIST, cryptography can be used to provide confidentiality, data integrity, authentication, authorization and non-repudiation. Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a key. The algorithm is a mathematical function, and the key is a parameter used in the transformation.

[91] *See* NISTIR 7628: Guidelines for Smart Grid Cyber Security and FIPS 140-2 for further guidance regarding smart grid systems and cryptography.

[92] *See* ISA/IEC-62443-2-1: Security for Industrial Automation and Control Systems - Industrial Automation and Control System Security Management System.

[93] *See* AGA 12: Cryptographic Protections for SCADA Communications.

[94] *See* NRC Regulatory Guide 5.71 for both data transmission integrity and confidentiality, as well as cryptographic key management.

variety of cryptographic tools, such as encryption, integrity checks, and multi-factor authentication, can enhance a responsible entity's defense-in-depth security strategies.

108. We are also concerned with NERC's proposal to exempt communication networks from protection based solely on specific types of technology. While proposed CIP-002-5 removes the prior blanket exemption for non-routable protocol, we seek comment regarding whether or not the resulting standards adequately protect non-routable communication systems.[95] We maintain our prior position that limiting the CIP protections to only routable systems adds additional risk to the bulk electric system.[96] Furthermore, by effectively locking the CIP Reliability Standards into a specific technology, we are concerned that any future technology which is non-routable in nature will not be addressed by the CIP Reliability Standards. Regardless of technology, the NIST Risk Management Framework addresses security for all communication systems.[97]

109. We invite comment on whether the adoption of communications security protections, such as cryptography and protections for non-routable protocol, would improve the CIP Reliability Standards.

---

[95] *See* NERC Petition at pages 11-12. In particular, CIP Version 5 introduces qualifying language for many requirements through the use of the "External Routable Connectivity" definition. Furthermore, other definitions exempt non-routable systems.

[96] *See* Order No. 761, 139 FERC ¶ 61,058 at PP 85-86.

[97] *See* SP 800-53 Revision 3, security control family System and Communications Protection, page F-106-123.

2. Remote Access

110. Remote access refers to the ability to access a non-public computer network from external locations.[98] Remote access provides greater flexibility in accessing remote computer networks; however, this flexibility creates new security risks by allowing a potentially unsecured device access into an entity's network.

111. Improperly implementing remote access procedures can create security vulnerabilities.[99] An entity must be able to verify that a party, whether it be an employee, vendor, or automated system, initiating remote access to the entity's internal networks has the appropriate access permissions. Since the communication network used for remote access is a pathway that can be used to spread malware, the secure implementation of remote access is another step in protecting the confidentiality, integrity, and availability of the data and functions used to support the reliable operation of the bulk electric system.

112. Due to the increased risk associated with utilizing remote access and the complexities involved with secure implementation, many groups have created guidance documents to aid in the secure implementation of remote access. NIST, Department of

---

[98] *See* SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security* page 2-1.

[99] *See* Remote Access VPN - Security Concerns and Policy Enforcement, SANS Reading Room, 2003, at page 3. *Available at* http://www.sans.org/reading_room/whitepapers/ vpns/remote-access-vpn-security-concerns-policy-enforcement_881

Homeland Security (DHS), and NERC have developed guidance documents for securing remote access connections.[100] The CIP version 5 Standards reflect certain aspects of these guidance documents. Specifically, proposed CIP-005-5, Requirement R2 requires responsible entities to utilize an Intermediate System, use encryption that terminates at an Intermediate System, and implement multi-factor authentication for all Interactive Remote Access sessions associated with high and medium impact BES Cyber Systems that allow Interactive Remote Access.[101]

113. The controls in CIP-005-5, Requirement R2, however, are not as stringent as the guidance in the NERC advisory or controls required under the NIST Risk Management Framework.[102] For example, both the NIST Risk Management Framework and NERC's remote access guidance document recommend authorization for each individual, person or system, granted remote access.[103] We invite comment on whether the adoption of more stringent controls for remote access would improve the CIP Reliability Standards.

---

[100] *See* SP 800-53 Revision 3, security control AC-17 page F-14-15. *See also* SP 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security. *See also* DHS *Configuring and Managing Remote Access for Industrial Control Systems. See also* NERC's *Guidance for Secure Interactive Remote Access.*

[101] *See* Petition at 12.

[102] *See* SP 800-53 Revision 3, security control AC-17, page F-14-15.

[103] *See* SP 800-53 Revision 3, security control AC-17, page F-14-15. See also *Guidance for Interactive Remote Access,* NERC, July 2011, page 12.

3. Differences Between the CIP Version 5 Standards and NIST

114. It appears 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. For example, certain security controls contained in NIST Special Publication 800-53's Security Control Catalog and associated guidance documents are not reflected in the CIP version 5 Standards.

115. The proposed CIP version 5 Standards do not address the proper upkeep and the protection of maintenance devices in as comprehensive a manner as the NIST Risk Management Framework.[104] In addition, proposed CIP-004-5 does not require a comprehensive analysis of all individual's duties to determine where separation of duties can be utilized to improve security.[105] The proposed CIP version 5 Standards also do not address the monitoring of information systems for new threats and vulnerabilities, as well as changes to how the asset should be categorized pursuant to CIP-002-5, in as comprehensive a manner as the NIST Risk Management Framework.[106]

---

[104] *See* SP 800-53 Revision 3, Maintenance and Media Protection control families, pages F-66 through F-75.

[105] *See* SP 800-53 Revision 3, control AC-5, pages F-8 and F-9.

[106] *See* SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* Page vi, "Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."

116. In particular, the CIP version 5 Standards do not provide for re-categorizing BES Cyber Systems based on a change in an individual entity's risk determinations. The CIP version 5 Standards also do not require minimum terms for contractual agreements associated with the acquisition or integration of new systems. [107] This is not an exhaustive list of the differences between the proposed CIP version 5 Standards and the NIST Risk Management Framework, but is representative of the differences in the security posture required under each.

117. While we are not proposing to direct NERC to address these concepts in the CIP Reliability Standards at this time, we invite 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.

IV. Information Collection Statement

118. The FERC-725B information collection requirements contained in this Proposed Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[108] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[109]

---

[107] *See generally* Department of Homeland Security: Cyber Security Procurement Language for Control Systems. See also SP 800-53 Revision 3, System and Services Acquisition control family, pages F-96 through F-105.

[108] 44 U.S.C. 3507(d) (2006).

[109] 5 CFR 1320.11 (2012).

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

119. The Commission based its paperwork burden estimates 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. While the Commission is proposing to allow the CIP version 3 Standards to remain in effect until the CIP version 4 Standards become effective, the Commission has already imposed the burden of implementing the CIP version 4 Standards. Thus, from a regulatory perspective, any change in burden related to the proposed approval of the CIP version 5 Standards would be relative to the change from the burden related to that imposed by the implementation of the CIP version 4 Standards.

120. The information collection burden under CIP version 5 is different than that imposed by CIP version 4. Under CIP version 4, all applicable entities must first identify, by applying criteria specified in CIP-002-4, which of the Cyber Assets they own are subject to the mandatory protections specified in the remaining CIP standards. Those

identified Cyber Assets are termed Critical Cyber Assets (CCA) in CIP version 4. If, upon completion of the required process in CIP-002-4, the entity has identified at least one CCA, it must implement all mandatory protections specified in the remaining CIP Reliability Standards with respect to any identified CCA. If, on the other hand, the entity determines that it does not own any CCAs, it is not required to implement any of the protections specified in the remaining CIP version 4 Standards. By contrast, CIP version 5 does not use the term CCA. Under CIP version 5, a responsible entity identifies Cyber Assets for protection by applying the CIP-002-5 definitions and classification criteria. The responsible entity is required to comply with at least some mandatory protections in the remaining standards for all Cyber Assets identified as BES Cyber Systems (depending on their classification of Low, Medium, or High and other specifics specified in various individual requirements).

121. Because the change in paperwork burden between CIP version 4 and CIP version 5 differs depending upon the extent to which that entity had to comply with CIP version 4, we delineate the registered entities into three groupings, as follows:

Group A: Entities that are not subject to the CIP version 4 Standards, but are subject to the CIP version 5 Standards. The Group A entities consist of those Distribution Providers that are not also registered for another CIP function, such as the Load Serving Entity function (which is subject to CIP version 4).

Group B: Entities that are registered for functions subject to CIP version 4, but that did not identify any CCAs under CIP-002-4. Therefore, Group B entities do not own

facilities that require the implementation of mandatory protections specified by the remaining CIP version 4 Standards.

Group C: Entities that are registered for functions subject to CIP version 4 *and* that identify, upon completion of the CIP-002-4 analysis, at least one asset as a CCA. Therefore, Group C entities own facilities that require the implementation of the mandatory protections specified in the remaining CIP version 4 Standards.

122. The NERC Compliance Registry as of February 28, 2013 indicated that 1,927 entities were registered for NERC's compliance program. Of these, 1,911 were identified as being U.S. entities. Staff concluded that of the U.S. entities, approximately 1,475 were registered for at least one CIP-applicable function, and therefore must comply with the CIP Reliability Standards. Further, 1,414 are subject CIP version 4. Consistent with the Commission's approach in Order No. 761,[110] we assume that 23 percent (325) of the 1,414 US entities subject to CIP version 4 identified CCAs (Group C). It follows that the remaining 77 percent (1089) of the US entities did not identify any CCAs under CIP version 4 (Group B). This ratio factors into several of the calculations needed to estimate the differences in effort among entities in Group B, as compared to Group C.

123. To estimate the change in paperwork burden between CIP version 4 and CIP version 5, we recognize that the entities in all groups will undertake the following paperwork tasks to at least some extent: 1) create or modify documentation of processes used to identify and classify the cyber assets to be protected under the CIP Reliability

[110] *See* Order No. 761, 139 FERC ¶ 61,058 at P 122, n.162.,

Standards; 2) create or modify policy, process and compliance documentation; and 3) continuing documentation of compliance data collection. We estimate the level of burden for each Group as follows:

- All of Group B & C entities, but no more than 10 percent of the Group A entities, will own at least one subject asset classified as Low under the CIP version 5 Standards. We estimate 24 hours[111] per entity to develop its evaluation process documentation for identifying the facilities subject to the standard, and 1,024 hours[112] to develop the required documentation for covered assets. We divide the total burden hours between the second and third years of the compliance period allowed for the assets classified as Low.
- The burden hours for facilities classified as Medium and High are split between the first and second year, since Groups B and C are allowed a 24-month period to bring them into compliance. (The third year figure shown for these rows represents an ongoing effort level). Except for Group C Blackstart facilities, 32 hours[113] per entity are assumed for development of its evaluation process documentation.

[111] Based on assumption of 2 persons per entity, working 15 percent of time for 2 weeks.

[112] Based on assumption of 2 persons per entity, creating required policy documentation per policy (4- low policies), working 40 percent of time for 8 weeks.

[113] Based on assumption of 2 persons per entity, working 20% of time for 2 weeks.

- We assume no more than 30 percent of Group B and Group C entities will own one or more of the newly covered transmission facilities classified as Medium. For those that do, we assume 3,200 hours [114] to develop the required policy, compliance and implementation documentation, and 832 hours [115] per entity for ongoing compliance burden.
- With respect to the Blackstart facilities owned by Group C entities, 160 hours [116] per entity are assumed for each entity to modify its policy and evaluation process documentation. We also assume a *reduction* of 728 hours [117] per entity for ongoing compliance documentation that is required under CIP version 4 but is no longer required under CIP version 5.

[114] Based on assumption of 1 person per entity, per standard (10) creating policy documentation, working 75 percent of time for 8 weeks, and 1 person per entity, per standard (10) on creating compliance documentation, 25 percent of time for 8 weeks.

[115] Based on assumption of 2 persons per entity, working 20 percent of time for 52 weeks.

[116] Based on assumption of 1 person per entity, per standard (10) modifying policy documentation, working 10 percent of time for 2 weeks, and 1 person per entity, per standard (10) modifying compliance documentation, 10 percent of time for 2 weeks.

[117] Based on assumption of a *reduction* of 2 persons per entity, collecting compliance data, working 20 percent of time for 52 weeks, and an *increase* of 1 person per entity, collecting compliance data, working 5 percent of time for 52 weeks.

- For Group C's Medium and High facilities, we assume 1,600 hours[118] per entity to modify the required policy, compliance and implementation documentation, and 416 hours[119] per entity for ongoing compliance.

124. The estimated paperwork burden changes for these entities, as contained in the proposed rule in RM13-5-000, are illustrated in the table below. The information collection burden also varies according to the types of facilities the entities own, as classified by the criteria in CIP-002-5, Attachment 1. To further refine our estimate, we indicate the classes of facilities each group of entities owns in the second column of the table below.

Groups of Registered Entities	Classes of Entity's Facilities Requiring V5 Protections	Number of Entities	Total Burden Hours in Year 1	Total Burden Hours in Year 2	Total Burden Hours in Year 3
Group A	Low[120]	61	0	3,804	3,804

[118] Based on assumption of 1 person per entity, per standard (10) modifying compliance documentation, working 50 percent of time for 8 weeks.

[119] Based on assumption of 2 persons collecting compliance data, working 10 percent of time for 52 weeks.

[120] Distribution Providers are the only functional entity type in Group A (*see* section 4, Applicability, of each CIP version 5 Standard), and their facilities are captured only by the Low classification criteria listed in CIP-002-5. The number of entities in this group represent the number of Distribution Providers that are not registered for any additional CIP version 5 applicable functions, including the Load Serving Entity function (and are therefore subject to CIP versions 1-4).

Group B	Low[121]	1,089	0	570,636	570,636
Group B	Medium[122]	260	128,960	128,960	64,896
Group C	Low[123]	325	0	170,300	170,300
Group C	Medium[124] (New)	78	1,248	1,248	19,136
Group C	Low[125]	283	22,640	22,640	-206,024

[121] As with Groups A and C, Group B will own Low facilities which were not identified for protections under prior CIP versions. The number of Group B respondents is calculated as 77 percent of the total entities previously subject to the CIP Reliability Standards. (.77 * 1414 = 1,089).

[122] In contrast to CIP version 4, Criterion 2.5 in CIP version 5 identifies new facilities for protection – transmission facilities =>200kV <300kV – and classifies them as "Medium." Some of these newly-applicable transmission facilities are owned by entities that had not previously identified any CCAs under previous versions, while some of the Criterion 2.5 facilities are owned by entities that previously identified CCAs. Assuming Group B entities constitute 77 percent of the entities to which this criterion potentially applies, 260 entities of the 338 total Transmission Owners (TO) captured by Criterion 2.5 are assigned to Group B, while the remaining 78 are allotted to Group C.

[123] As with Groups A and B, the entities that identified CCAs under CIP version 4 (Group C) will also own facilities newly addressed by CIP version 5 and classified as Low. The number of Group B respondents is calculated as 23 percent of the total entities previously subject to the CIP Reliability Standards. (.23 * 1414 = 325)

[124] This row concerns only the newly subject transmission facilities that are addressed by CIP version 5, Criterion 2.5, as owned by Group C TO entities. *See* the note for Group B Medium above for further explanation. These Medium-rated facilities are broken out in this row, separate from other Medium facilities the entity may own in the High and Medium row below because the level of effort for these Group C TOs entities to protect these newly protected facilities is estimated differently than for the Group B entities, or for other Medium facilities the entity may own.

[125] Blackstart generation and transmission cranking paths are the only types of facilities identified first for more specified security controls under CIP version 4, Criteria

(continued…)

	(Blackstart)				
Group C	Medium or High[126]	325	265,200	265,200	135,200
Totals			418,048	1,163,556	758,716

125. The following shows the average annual cost burden for each group, based on the burden hours in the table above:[127]

- 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

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

126. 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

---

1.4 and 1.5, but then subject only to Low mandatory security controls under CIP version 5, Criterion 3.4. The number of entities in this row represents 23 percent of the sum of all registered Generation Operators to account for Blackstart Resources and all TOs to account for cranking paths.

[126] Except for the Blackstart facilities noted above, the facilities that Group C entities identify as CCAs under CIP version 4 will be rated for Medium or High security controls under CIP version 5.

[127] The total cost figures are rounded to the nearest thousand. The "hours per entity" figures are averages over three years for the whole group. Some entities within a group may experience higher or lower hourly impact (as illustrated in the burden table) depending on entity type and assets owned.

administrative support ($30.18 per hour), based on hourly rates and average benefits data from the Bureau of Labor Statistics.[128]

127. Title: Mandatory Reliability Standards, Version 5 Critical Infrastructure Protection Standards

Action: Proposed Collection FERC-725B.

OMB Control No.: 1902-0248.

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

Frequency of Responses: On Occasion.

Necessity of the Information: This proposed rule proposes to approve the requested modifications to Reliability Standards pertaining to critical infrastructure protection. The proposed 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 proposes to approve NERC's proposed Version 5 CIP Standards pursuant to section 215(d)(2) of the FPA because they represent an improvement to the currently-effective CIP Reliability Standards.

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

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.

128. 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].

129. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM13-5-000 and OMB Control Number 1902-0248.

V. Regulatory Flexibility Act Certification

130. The Regulatory Flexibility Act of 1980 (RFA)[129] generally requires a description and analysis of proposed 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

[129] 5 U.S.C. 601-612 (2006).

Administration's Office of Size Standards develops the numerical definition of a small business.[130] The Small Business Administration 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, 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 (MWh).[131]

131. The Commission seeks comment on the estimated impact of implementing and complying with the CIP version 5 Reliability Standards. Specifically, the Commission seeks detailed and supported information regarding the impacts in order to better estimate the cost on small businesses.

132. The Commission estimates the NOPR will impact 536 small entities.[132] Of this amount, the Commission estimates that only 14 small entities[133] (2.6 percent of the total number of 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

[130] 13 CFR 121.101 (2012).

[131] 13 CFR 121.201, Sector 22, Utilities & n.1.

[132] Based on a comparison of the NERC Compliance Registry (as of February 28, 2013) and Energy Information Administration Form 861 (*available at* http://www.eia.gov/electricity/data/eia861/index.html)

[133] The 14 small entities in this class represent small Transmission Owners assumed to fall under the Medium classification and thus experience a greater impact than other small entities. These same entities also experience the impact associated with the Low classification.

year.[134] This cost is primarily due to implementation during the compliance period. After the initial implementation the Commission expects the average annual cost per each of the 14 entities to be less than $64,000. The Commission has determined that 2.6 percent of the effected small entities do not represent a "substantial number" in terms of the total number of regulated small entities applicable to the NOPR.

133. The Commission estimates that 234 out of the 536 small entities[135] will each experience an average economic impact of $29,000 per year during years two and three.[136] Finally, the Commission estimates that the remaining 288 out of the 536 small entities[137] will only experience a minimal economic impact.

134. Based on the above, the Commission certifies that the proposed Reliability Standards will not have a significant impact on a substantial number of small entities. Accordingly, no initial regulatory flexibility analysis is required.

---

[134] These costs are 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.

[135] This figure represents the number of small entities that own assets covered by CIP version 5. This number does not include the 14 significantly impacted entities.

[136] This cost figure is 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.

[137] The number of small Distribution Providers assumed to not own assets covered by CIP version 5.

VI. Environmental Analysis

135. 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.[138] 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.[139] The actions proposed here fall within this categorical exclusion in the Commission's regulations.

VII. Comment Procedures

136. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due [INSERT DATE 60 days after publication in the **FEDERAL REGISTER**]. Comments must refer to Docket No. RM13-5-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

137. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts

---

[138] *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).

[139] 18 CFR 380.4(a)(2)(ii).

most standard word processing formats. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

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

139. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

VIII. Document Availability

140. 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.

141. 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.

142. 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.

By direction of the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.