136 FERC ¶ 61,184
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

Docket No. RM11-11-000

Version 4 Critical Infrastructure Protection Reliability Standards

(September 15, 2011)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: Under section 215 of the Federal Power Act, the Federal Energy Regulatory Commission (Commission) proposes to approve eight modified Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-4 through CIP-009-4, developed and submitted to the Commission for approval by the North American Electric Reliability Corporation (NERC), the Electric Reliability Organization certified by the Commission. In general, the CIP Reliability Standards provide a cybersecurity framework for the identification and protection of "Critical Cyber Assets" to support the reliable operation of the Bulk-Power System. Proposed Reliability Standard CIP-002-4 requires the identification and documentation of Critical Cyber Assets associated with Critical Assets that support the reliable operation of the Bulk-Power System. The "Version 4" CIP Reliability Standards propose to modify CIP-002-4 to include "bright line" criteria for the identification of Critical Assets. The proposed Version 4 CIP Reliability Standards would replace the currently effective Version 3 CIP Reliability Standards. The Commission also proposes to approve the related Violation Risk Factors

and Violation Severity Levels with modifications, the implementation plan, and effective date proposed by NERC.

DATES: Comments are due [Insert date that is 60 days after publication in the **FEDERAL REGISTER**].

ADDRESSES: You may submit comments, identified by docket number and in accordance with the requirements posted on the Commission's website http://www.ferc.gov. Comments may be submitted by any of the following methods:

- Agency Web Site: Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format, at http://www.ferc.gov/docs-filing/efiling.asp.
- Mail/Hand Delivery: Commenters unable to file comments electronically must mail or hand deliver an original copy of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426. These requirements can be found on the Commission's website, see, e.g., the "Quick Reference Guide for Paper Submissions," available at http://www.ferc.gov/docs-filing/efiling.asp or via phone from FERC Online Support at 202-502-6652 or toll-free at 1-866-208-3676.

FOR FURTHER INFORMATION CONTACT:

Jan Bargen (Technical Information)
Office of Electric Reliability
Division of Logistics and Security
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6333

Edward Franks (Technical Information)
Office of Electric Reliability
Division of Logistics and Security
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6311

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

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

SUPPLEMENTARY INFORMATION:

136 FERC ¶ 61,184
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Version 4 Critical Infrastructure Protection Reliability Standards — Docket No. RM11-11-000

NOTICE OF PROPOSED RULEMAKING

(September 15, 2011)

1. Under section 215 of the Federal Power Act (FPA),[1] the Commission proposes to approve eight modified Critical Infrastructure Protection (CIP) Reliability Standards, CIP-002-4 through CIP-009-4. The proposed "Version 4" CIP Standards were developed and submitted for approval to the Commission by the North American Electric Reliability Corporation (NERC), which the Commission certified as the Electric Reliability Organization (ERO) responsible for developing and enforcing mandatory Reliability Standards.[2] In general, the CIP Reliability Standards provide a cybersecurity framework for the identification and protection of "Critical Cyber Assets" to support the reliable operation of the Bulk-Power System.[3] In particular, the Version 4 CIP Reliability Standards propose to modify CIP-002-4 to include "bright line" criteria for the identification of Critical Assets, in lieu of the currently-required risk-based assessment

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

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

[3] The NERC Glossary of Terms defines Critical Assets to mean "Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."

methodology that is developed and applied by applicable entities. In addition, NERC developed proposed conforming modifications to the remaining cybersecurity Reliability Standards, CIP-003-4 through CIP-009-4.

2. The Commission proposes to approve Version 4, the Violation Risk Factors (VRFs),the Violation Severity Levels (VSLs) with modifications, the implementation plan, and effective date proposed by NERC. The Commission also proposes to approve the retirement of the currently effective Version 3 CIP Reliability Standards, CIP-002-3 to CIP-009-3. The Commission seeks comments on these proposals to approve.

3. While we propose to approve the Version 4 CIP Standards, like NERC, we recognize that the Version 4 CIP Standards represent an "interim step"[4] to addressing all of the outstanding directives set forth in Order No. 706.[5] We believe that the electric industry, through the NERC standards development process, should continue to develop an approach to cybersecurity that is meaningful and comprehensive to assure that the nation's electric grid is capable of withstanding a Cybersecurity Incident.[6] Below, we reiterate several topics set forth in Order No. 706 that pertain to a tiered approach to identifying Cyber Assets, protection from misuse, and a regional perspective. We expect

[4] NERC Petition at 6.

[5] *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).

[6] Section 215(a) of the FPA defines Cybersecurity Incident as "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."

NERC will continue to improve the CIP Standards to address these and other outstanding matters addressed in Order No. 706.

4. Moreover, as discussed below, the Commission seeks comments from NERC and other interested persons on establishing a reasonable deadline for NERC to satisfy the outstanding directives in Order No. 706 pertaining to the CIP Standards, using NERC's development timeline.

I. Background

A. Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[7]

6. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO[8] and, subsequently, certified NERC as the ERO.[9] On January 18, 2008, the Commission issued Order No. 706 approving eight CIP Reliability Standards proposed by NERC.

---

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

[8] *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).

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

7. In addition, pursuant to section 215(d)(5) of the FPA,[10] the Commission directed NERC to develop modifications to the CIP Reliability Standards to address various concerns discussed in the Final Rule. In relevant part, the Commission directed the ERO to address the following issues regarding CIP-002-1: (1) need for ERO guidance regarding the risk-based assessment methodology for identifying Critical Assets; (2) scope of Critical Assets and Critical Cyber Assets; (3) internal, management, approval of the risk-based assessment; (4) external review of Critical Assets identification; and (5) interdependency between Critical Assets of the Bulk-Power System and other critical infrastructures. Subsequently, the Commission approved Version 2 and Version 3 of the CIP Reliability Standards, each version including changes responsive to some but not all of the directives in Order No. 706.[11]

B. Current Version 3 CIP Reliability Standards

8. Reliability Standard CIP-002-3 addresses the identification of Critical Assets and associated Critical Cyber Assets. Pursuant to CIP-002-3, a responsible entity must develop a risk-based assessment methodology to identify its Critical Assets. Requirement R1 specifies certain types of assets that an assessment must consider for Critical Asset status and also allows the consideration of additional assets that the responsible entity deems appropriate. Requirement R2 requires the responsible entity to

[10] 16 U.S.C. 824o(d)(5).

[11] *North American Electric Reliability Corp*., 128 FERC ¶ 61,291 (2009), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving Version 2 of the CIP Reliability Standards); *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010) (approving Version 3 of the CIP Reliability Standards).

develop a list of Critical Assets based on an annual application of the risk-based assessment methodology developed pursuant to Requirement R1. Requirement R3 provides that the responsible entity must use the list of Critical Assets to develop a list of associated Critical Cyber Assets that are essential to the operation of the Critical Assets.

9. In addition, the Commission approved the following "Version 3" CIP Standards:

- CIP-003-3 (Security Management Controls)
- CIP-004-3 (Personnel & Training)
- CIP-005-3 (Electronic Security Perimeter(s))
- CIP-006-3 (Physical Security of Critical Cyber Assets)
- CIP-007-3 (Systems Security Management)
- CIP-008-3 (Incident Reporting and Response Planning)
- CIP-009-3 (Recovery Plans for Critical Cyber Assets)

II. Proposed Version 4 CIP Reliability Standards

A. NERC Petition

10. On February 10, 2011, NERC filed a petition seeking Commission approval of proposed Reliability Standards CIP-002-4 to CIP-009-4 and requesting the concurrent retirement of the currently effective Version 3 CIP Reliability Standards, CIP-002-3 to CIP-009-3.[12] The principal differences are found in CIP-002, where NERC replaced the

[12] NERC Petition at 1. The proposed Reliability Standards are not attached to the NOPR. They are, however, available on the Commission's eLibrary document retrieval system in Docket No. RM11-11-000 and are available on the ERO's website, www.nerc.com. Reliability Standards approved by the Commission are not codified in the CFR.

risk-based assessment methodology for identifying Critical Assets with 17 uniform bright line criteria for identifying Critical Assets. NERC does not propose any changes to the process of identifying the associated Critical Cyber Assets that are then subject to the cyber security protections required by CIP-003 through CIP-009. NERC also submitted proposed VRFs and VSLs and an implementation plan governing the transition to Version 4. NERC proposed that the Version 4 CIP Reliability Standards become effective the first day of the eighth calendar quarter after applicable regulatory approvals have been received.

11. On April 12, 2011, NERC made an errata filing correcting certain errors in the petition and furnishing corrected exhibits and the standard drafting team minutes. In the errata, NERC also replaced the VRFs and VSLs in the February 10 petition with new proposed VRFs and VSLs.[13]

12. In its Petition, NERC states the that Version 4 CIP Standards satisfy the Commission's criteria, set forth in Order No. 672, for determining whether a proposed Reliability Standard is just, reasonable, not unduly discriminatory or preferential and in

[13] NERC states that the Version 4 VRFs and VSLs are carried over in part from the VRFs and VSLs in the Version 3 CIP Reliability Standards. NERC Petition at 46. The Commission approved the Version 2 and 3 VRFs and VSLs in Docket Nos. RD10-6-001 and RD09-7-003 on January 20, 2011 but required NERC to make modifications in a compliance filing due by March 21, 2011. *North American Electric Reliability Corporation*, 134 FERC ¶ 61,045 (2011). The February 10 petition did not carry over the modified Version 3 VRFs and VSLs since it was filed before the March 21 compliance filing. NERC submitted new Version 4 VRFs and VSLs that carried over the modified Version 3 VRFs and VSLs in the April 12 errata. On June 6, 2011, NERC filed the March 21, 2011 compliance filing in the present docket, Docket No. RM11-11-000.

the public interest.[14] According to NERC, CIP-002-4 achieves a specified reliability goal by requiring the identification and documentation of Critical Cyber Assets associated with Critical Assets that support the reliable operation of the Bulk-Power System. NERC opines that the Reliability Standard "improves reliability by establishing uniform criteria across all Responsible Entities for the identification of Critical Assets."[15] Further, NERC states that CIP-002-4 contains a technically sound method to achieve its reliability goal by requiring the identification and documentation of Critical Assets through the application of the criteria set forth in Attachment 1 of CIP-002-4.

13. NERC states that CIP-002-4 establishes clear and uniform criteria for identifying Critical Assets on the Bulk-Power System.[16] NERC also states that CIP-002-4 does not reflect any differentiation in requirements based on size of the responsible entity. NERC asserts that CIP-002-4 will not have negative effects on competition or restriction of the grid. NERC also contends that the two-year implementation period for CIP-002-4 is reasonable given the time it will take responsible entities to determine whether assets meet the criteria included in Attachment 1 and to implement the controls required in CIP-003-4 through CIP-009-4 for the newly identified assets.

14. Finally, NERC acknowledges that CIP-002-4 addresses some, but not all, of the Commission's directives in Order No. 706. NERC explains that the standard drafting team limited the scope of requirements in the development of CIP Version 4 "as an

---

[14] Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 323-337.

[15] NERC Petition at 4.

[16] *Id.* at 38.

interim step" limited to the concerns raised by the Commission regarding CIP-002.[17] NERC states that it has taken a "phased" approach to meeting the Commission's directives from Order No. 706 and, according to NERC, the standard drafting team continues to address the remaining Commission directives. According to NERC, the team will build on the bright line approach of CIP Version 4.[18]

B. Proposed Reliability Standard CIP-002-4

15. Proposed Reliability Standard CIP-002-4 contains 3 requirements. Requirement R1, which pertains to the identification of Critical Assets, provides:

> The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall update this list as necessary, and review it at least annually.

Attachment 1 provides seventeen criteria to be used by all responsible entities for the identification of Critical Assets pursuant to Requirement R1. The thresholds pertain to specific types of facilities such as generating units, transmission lines and control centers. For example, Criterion 1.1 provides "[e]ach group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW in a single Interconnection." With regard to transmission, Criterion 1.6 provides "Transmission Facilities operated at 500 kV or higher," and Criterion 1.7 provides "Transmission

[17] NERC Petition at 6 (citing Order No. 706, 122 FERC ¶ 61,040 at P 236).

[18] NERC Petition at 6.

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

16. Reliability Standard CIP-002-4, Requirement R2 requires responsible entities to develop a list of Critical Cyber Assets associated with the Critical Assets identified pursuant to Requirement R1. As in previous versions, the Requirement further states that to qualify as a Critical Cyber Asset, the Cyber Asset must: (1) use a routable protocol to communicate outside the Electronic Security Perimeter; (2) use a routable protocol within a control center; or (3) be dial-up accessible. In the proposed version, in the context of generating units at a single plant location, the Requirement limits the designation of Critical Cyber Assets only to Cyber Assets shared by a combination of generating units whose compromise could within 15 minutes result in the loss of generation capability equal to or higher than 1500 MW.

17. Requirement R3 requires that a senior manager or delegate for each responsible entity approve annually the list of Critical Assets and the list of Critical Cyber Assets, even if the lists contain no elements. As mentioned above, proposed Reliability Standards CIP-003-4 to CIP-009-4 only reflect conforming changes to accord with the CIP-002-4 Reliability Standard.

C. Additional Information Regarding Attachment 1 Criteria

18. In response to a Commission data request, NERC provided additional information regarding the bright line criteria for identifying Critical Assets.[19] NERC provided some

[19] *See* April 17, 2011 Commission staff data request issued in Docket No. RM11-11-000. NERC responded to the data request in staggered filings, on May 27, 2011 and

information regarding the development of the criteria. Further, based on an industry survey, NERC provided information regarding the estimated number of Critical Assets and the number of Critical Assets that have associated Critical Cyber Assets located in the United States that would be identified pursuant to CIP-002-4. For example, NERC indicates that the Version 4 CIP Standards would result in the identification of 532 control centers as Critical Assets with Critical Cyber Assets, and another 21 control centers as Critical Assets without any associated Critical Cyber Assets.[20] Further, 201 control centers would not be identified as Critical Assets. With regard to Blackstart Resources, NERC's survey results indicate that CIP-002-4 would result in the identification of approximately 234 Blackstart Resources as Critical Assets with associated Critical Cyber Assets, 273 identified as Critical Assets without Critical Cyber Assets, and 35 Blackstart Resources not classified as Critical Assets.[21]

III. Discussion

19. Pursuant to FPA section 215(d)(2), the Commission proposes to approve CIP-002-4 to CIP-009-4 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission proposes to approve the VRFs and VSLs, implementation plan, and effective date proposed by NERC. The Commission also proposes to approve the retirement of the currently effective Version 3 CIP Reliability

---

June 30, 2011.

[20] NERC June 30, 2011 Data Response at 2-3.

[21] *Id*. at 3-4. In the June 30, 2011 Data Response, NERC stated that with respect to Blackstart Resources some responsible entities indicated that they had not performed a complete analysis of their systems based on CIP-002-4 and are unsure whether some units may be classified as Critical Assets. *Id.* at 4.

Standards CIP-002-3 to CIP-009-3 upon the effective date of CIP-002-4 to CIP-009-4. The Commission seeks comments on these proposals.

20. Further, as discussed below, the Commission seeks comments from NERC and other interested persons on the proposal to establish a reasonable deadline for NERC to satisfy the outstanding directives in Order No. 706. Specifically, as explained in detail later, the Commission requests comments on: (1) the proposal to establish a deadline using NERC's development timeline for the next version of the CIP Reliability Standards; (2) how much time NERC needs to develop and file the next version of the CIP Reliability Standards; (3) other potential approaches to Critical Cyber Asset identification; and (4) whether the next version is anticipated to satisfy all of the directives in Order No. 706.

A. The Commission Proposes to Approve the Version 4 CIP Reliability Standards

21. The Commission, in giving due weight to NERC's Filing, proposes to approve the Version 4 CIP Reliability Standards. The Commission also proposes to approve the implementation plan and effective date proposed by NERC. Version 4 provides a change in three respects: (1) Version 4 will result in the identification of certain types of Critical Assets that may not be identified under the current approach; (2) Version 4 uses bright line criteria to identify Critical Assets, eliminating the use of existing entity-defined risk-based assessment methodologies that generally do not adequately identify Critical Assets; and (3) Version 4 provides a level of consistency and clarity regarding the identification

of Critical Assets lacking under Version 3. We separately address each of these reasons for proposing to approve Version 4 below.

1. Critical Asset Identification

22. In its Petition, NERC indicates that, after conducting reviews of CIP-002 compliance, NERC "determined that the existing methodologies generally do not adequately identify all Critical Assets."[22] While recognizing that CIP version 4 is intended as an "interim step," it appears that the proposed bright line criteria will result in the identification of certain types of Critical Assets (e.g. 500 kV substations) that may not be identified by the approach that is currently in effect. This is reflected in NERC's June 30, 2011 data response, in which NERC presented industry survey data reflecting the application of the bright line criteria in Version 4. To facilitate an analysis of the data, NERC also provided observations and data from several of its earlier industry surveys, including the 2009 "CIP Self-Certification Survey" and 2010 "CIP-002 Critical Asset Methodology Data Request.". For example, NERC states in the June 30, 2011 data response that in the 2009 survey only 50 percent of substations rated 300 kV and above are classified as Critical Assets while that figure would increase to 70 percent under Version 4.[23]

23. The NERC petition indicates that 270 transmission substations rated 500 kV and above are classified as Critical Assets under Version 3 while, according to the data

[22] NERC Petition at 11

[23] *Id*. at 4.

response, the figure would rise to 437 under Version 4.[24] This increase is consistent with Criterion 1.6 of Attachment 1 to CIP-002-4, which identifies all transmission substations rated 500 kV as Critical Assets. According to the data response, the 25 percent of generation units rated 300 MVA and above would be identified as Critical Assets under Version 4. Moreover, the proportion of total Blackstart Resources classified as Critical Assets increases due to the required 100 percent coverage of these under Version 4.[25] Further, the number of control centers identified as Critical Assets increases from 425 under Version 3 to 553 under Version 4, the latter figure representing 74 percent of all control centers. These figures represent increases in certain categories in Critical Asset identification among generation, transmission, and control centers. We also note that NERC's industry survey data indicates decreases in the number of generation and blackstart resources identified as Critical Assets with Critical Cyber Assets. While the bright line thresholds result in the identification of a significant number of additional generation plants rated above 1500 MVA as Critical Assets, the thresholds also result in the identification of less generation below 300 MVA.

24. As NERC recognizes in its filing, the improvements in Critical Asset identification under Version 4 represent an interim step in complying with the directives in Order

[24] *Id.* at 5.

[25] NERC Petition at 17 (explaining that each Blackstart Resource identified in a Transmission Operator's restoration plan is a Critical Asset). In the June 30, 2011 Data Response, NERC's survey found that responsible entities identified 93 percent of Blackstart Resources as Critical Assets. NERC stated that confusion over the term Blackstart Resource may have contributed to the lower percentage, and that responsible entities will be educated on the definition of Blackstart Resource prior to the effective date of CIP-002-4. NERC June 30, 2011 Data Response at 4.

No. 706.[26] As we discuss below, Version 4 should not be viewed as an endpoint but as a step towards eventual full compliance with Order No. 706.

2. Version 4 Removes Discretion in Identifying Critical Assets

25. The proposed Version 4 CIP Reliability Standards discards the current risk-based methodology for identifying Critical Assets. Under the current CIP-002-3, responsible entities are tasked with identifying Critical Assets based on their own risk-based methodology. In the Petition NERC points out that in Order No. 706 the Commission directed NERC to "provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System."[27] NERC explains that it responded to the Commission's direction by developing guidance documents to assist entities in developing their risk-based methodologies and Critical Asset identification.[28]

26. In its Petition, NERC states that it "conducted various reviews of risk-based methodologies developed by many entities of varying sizes . . . and determined that the existing methodologies generally do not adequately identify all Critical Assets."[29] To address this, NERC proposes to replace the current risk-based methodology with uniform, bright line criteria, which will be used by all responsible entities to identify Critical Assets.

---

[27] *Id.* at 10-11 (citing Order No. 706, 122 FERC ¶ 61,040 at P 255).

[28] *Id.* at 11.

[29] *Id.*

27. While risk-based assessment methodologies have merit, we share NERC's concerns about the existing application of the currently effective CIP-002-3, Requirement 1. Thus, in this context, we believe that a shift away from responsible entity-designed risk-based methodologies for identifying Critical Assets, which NERC has found to be inadequate, to the use of NERC-developed criteria is an improvement.

3. Version 4 Provides Consistency and Clarity in the Identification of Critical Assets

28. In its June 30, 2011 data response, NERC states that the survey results from 2009 generated concern "about the apparent inconsistency in the application of the standards across the system, as evidenced by the apparent variation from region to region."[30] NERC states that it subsequently engaged with the Regional Entities and stakeholders to better understand the data, with these efforts resulting in the development of Version 4.

29. We believe that the application of uniform criteria is an improvement over the current approach because they add greater consistency and clarity in identifying Critical Assets. The risks posed by cyber threats suggest a different approach than the possibly inconsistent, inadequate methodologies for identifying Critical Assets, as evidenced by NERC's conclusion that insufficient numbers of Critical Assets were identified using the risk-based assessment methodology. As an integrated system, the protection afforded for Critical Assets and their Critical Cyber Assets is only as strong as its weakest link. In this respect, allowing responsible entities to devise their own methodologies for identifying Critical Assets, especially if these methodologies prove to be weak, may

[30] NERC June 30, 2011 Data Response at 3.

compromise the Critical Assets and Critical Cyber Assets of other responsible entities even if they have adopted a more stringent methodology. The uniform system of Critical Asset identification proposed by NERC in Version 4 helps to address this weakness and places all responsible entities on an equal footing with respect to Critical Asset identification.

30. In addition, clear, bright line criteria should make it easier for Regional Entities, NERC and the Commission to monitor responsible entities and evaluate how they are identifying Critical Assets. A single set of bright line criteria, as opposed to myriad entity-designed risk-based methodologies, should improve the CIP compliance process.

31. However, under the currently-effective CIP-002-3, an entity that applies its risk-based assessment methodology considers specific types of assets identified in Requirement R1, as well as "any additional assets that support the operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment." Thus, currently, a responsible entity has the flexibility to consider any assets it deems appropriate. The Commission also notes that there are assets currently identified as Critical Assets which would no longer be identified as Critical Assets under the Proposed Reliability Standard CIP-002-4 bright line criteria for Critical Asset identification. The Commission seeks comment whether, under CIP Version 4, a responsible entity retains the flexibility to identify assets that, although outside of the bright line criteria, are essential to Bulk-Power System reliability. Further, we seek comment whether the ERO and/or Regional Entities would have the ability, either in an event-driven investigation or compliance audit, to identify specific assets that fall outside

the bright-line criteria yet are still essential to Bulk-Power System reliability and should be subject prospectively to compliance with the CIP Reliability. If so, on what basis should that decision be made?

32. In addition, the Commission is cognizant of one caution that remains concerning a binary bright line criteria protection philosophy, *i.e.*, either an asset satisfies the threshold and is subject to compliance or is below the threshold and not subject to compliance (as opposed to a tiered approach to compliance as discussed below), in terms of applying cybersecurity protections to Cyber Assets. Specifically, bright line criteria that limit legally-mandated cybersecurity protections to certain classes of Bulk-Power System assets may indicate to an adversary the types of assets that fail to meet the threshold and, therefore, are not subject to mandatory CIP compliance. Therefore, the Commission encourages NERC to accelerate development of the next version of the CIP Reliability Standards and to address the concerns discussed herein in Section B.

4. Violation Risk Factors/Violation Severity Levels

33. NERC states that the proposed VRFs and VSLs are consistent with those approved for the Version 3 CIP Reliability Standards.[31] NERC explains that each requirement in Version 4 is assigned a VRF and a set of VSLs and that these elements support the determination of an initial value range for the base penalty amount regarding violations

[31] *North American Electric Reliability Corp.*, 134 FERC ¶ 61,045 (2011) (approving Version 2 and 3 CIP Reliability Standards VRFs and VSLs but requiring modifications in a compliance filing).

of requirements in Commission-approved Reliability Standards, as defined in the ERO Sanction Guidelines.[32]

34. The principal changes in the proposed Version 4 VRFs and VSLs relate to CIP-002-4. NERC proposes to carry forward the Version 3 VRFs and VSLs for all other Requirements (in CIP-003-4 through CIP-009-4), for which no substantive revisions are proposed. CIP-002-4 no longer contains sub-Requirements and, instead, each of three main Requirements has a single VRF and set of VSLs, consistent with the methodology proposed by NERC and approved by the Commission.[33] The VRF designations for the three Requirements in CIP-002-4 are consistent with those assigned to similar Requirements in previous versions of the CIP Reliability Standards and satisfy our established guidelines. Therefore, the Commission proposes to approve the Version 4 VRFs proposed by NERC and incorporate appropriately the modifications directed to prior versions.

35. With regard to the proposed Version 4 VSLs for CIP-002-4, we are concerned that the VSLs for Requirement R1 and Requirement R2, while carrying forward the wording from corresponding Version 3 VSLs, do not adequately address the purpose of NERC's proposed bright line criteria: to ensure accurate and complete identification of all Critical Assets, so that all associated Critical Cyber Assets become subject to the protections required by the CIP Standards.

---

[32] NERC Petition at 37.

[33] *North American Electric Reliability Corp.*, 135 FERC ¶ 61,166, at 8 (2011).

36. More importantly, neither set of VSLs address the failure to properly identify either Critical Assets or Critical Cyber Assets in the first place. The failure to identify a Critical Asset, whether inadvertently or through misapplication of the bright line criteria, is paramount because if an Asset is not identified and included on the Critical Asset list, its associated Cyber Assets will not be considered under Requirement R2. Failure to identify those Cyber Assets as Critical Cyber Assets under Requirement R2 then creates the "weakest link" circumstance discussed in the Commission's order establishing two CIP VSL Guidelines for analyzing the validity of VSLs pertaining to cyber security.[34]

37. Therefore, the Commission proposes to direct the ERO to modify the VSLs for CIP-002-4, Requirements R1 and R2, to address a failure to identify either Critical Assets or Critical Cyber Assets, as shown in Appendix 1.[35] The Commission proposes to approve the Version 4 VSLs proposed by NERC, as modified, because they would then satisfy our established guidelines, fully address the purpose of NERC's bright line criteria, and incorporate appropriately the modifications directed to prior versions.

---

[34] CIP VSL Guideline 1 states, "Requirements where a single lapse in protection can compromise computer network security, i.e., the "weakest link" characteristic, should apply binary rather than gradated VSLs."

[35] NERC proposes to assign a Severe VSL for a violation of Requirement R1 if a responsible entity does not develop a list of its identified Critical Assets "even if such list is null." NERC does not propose to assign a VSL for a violation of Requirement R1 when a responsible entity fails to identify a Critical Asset that falls within any of the Critical Asset Criteria in Attachment 1, or fails to include an identified Critical Asset in its Critical Asset list. NERC further proposes to assign a Severe VSL to a responsible entity's violation of Requirement R2 only when it fails to include in its list of Critical Cyber Assets a Critical Cyber Asset it has identified. NERC does not propose to assign a VSL for a violation of Requirement R2 resulting from a responsible entity's failure to identify as a Critical Cyber Asset a Cyber Asset that qualifies as a Critical Cyber Asset.

5. Implementation Plan and Effective Date

38. NERC proposes an effective date for full compliance with the Version 4 CIP Standards of the first day of the eighth calendar quarter after applicable regulatory approvals have been received. In addition, NERC provides a detailed implementation plan for newly identified Critical Assets and newly registered entities. NERC also presents a number of scenarios intended to explain how CIP-002-4 will be implemented. Depending on the situation, the implementation plan establishes timelines and milestones for entities to reach full compliance with CIP-002-4.

39. The Commission proposes to approve the effective date and implementation plan for CIP-002-4. Under the scenarios presented by NERC, we understand that entities with existing CIP compliance implementation programs will effectively no longer use CIP-002-3 to identify Critical Assets after approval of CIP-002-4 but rather will apply the criteria in Attachment 1 of CIP-002-4. While some responsible entities have already installed the necessary equipment and software to address cybersecurity, we recognize that other responsible entities may need to purchase and install new equipment and software to achieve compliance for assets that are brought within the scope of the protections under the CIP-002-4 bright line criteria. Based on these considerations, the Commission believes that the implementation plan proposed by NERC sets reasonable deadlines for industry compliance.

B. Ongoing Development Efforts to Satisfy Directives Set Forth in Order No. 706

40. As acknowledged by NERC, the proposed Version 4 CIP Reliability Standards do not address all of the directives set forth in Order No. 706. Although the Commission proposes to approve CIP-002-4, we highlight the need for NERC, working through the Reliability Standards development process, to address all outstanding Order No. 706 directives as soon as possible.

41. Below, we discuss several directives in Order No. 706 that have yet to be satisfied and propose to give guidance regarding the next version of the CIP Reliability Standards, such as the need to address the NIST framework, data network connectivity, and the potential misuse of control centers or control systems and the adoption of a regional perspective and oversight. Our guidance is intended to more fully ensure that all Cyber Assets serving reliability functions of the Bulk-Power System are within scope of the CIP Reliability Standards. In addition, as discussed below, we seek comments from NERC and other interested persons on a proposal to establish a deadline for NERC to submit modified CIP Reliability Standards that address the outstanding directives set forth in Order No. 706, using NERC's development timeline.

42. The stated purpose of Reliability Standard CIP-002 is the accurate identification of Critical Cyber Assets. Both the currently-effective and proposed CIP-002 Reliability

Standards, along with guidance NERC provided to industry,[36] are structured in a staged approach. First, an entity must identify Critical Assets. NERC defines Critical Assets as "facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System."[37] Second, based on the Critical Assets identified in the first step, an entity must identify Cyber Assets supporting the Critical Assets. The NERC Glossary defines Cyber Assets as "programmable electronic devices and communication networks including hardware, software, and data."[38] Third, an entity should identify the Critical Cyber Assets by determining, in accordance with the NERC Glossary, the "Cyber Assets essential to the reliable operation of the Critical Assets."[39] In Order No. 706, the Commission did not address whether or not the staged approach outlined above was the only method for identifying Critical Cyber Assets. Rather at that time, focus was placed on addressing specific concerns with the first step – the identification of Critical Assets. Recognizing CIP-002 as the cornerstone of the CIP Reliability Standards,[40] a failure to accurately identify Critical Assets could greatly impact accurate Critical Cyber Asset identification

[36] North American Reliability Corporation Security Guideline for the Electric Sector: "*Identifying Critical Cyber Assets*" Version 1.0, Effective June 17, 2010, at 4-5, and North American Reliability Corporation Security Guideline for the Electric Sector: "*Identifying Critical Assets*" Version 1.0, Effective September 17, 2009.

[37] NERC Glossary of Terms at 11.

[38] *Id.*

[39] *Id.*

[40] Order No. 706, 122 FERC ¶ 61,040 at P 234.

and the overall applicability of the protection measures afforded in CIP-003 through CIP-009.

43. In light of recent cybersecurity vulnerabilities, threats and attacks that have exploited the interconnectivity of cyber systems,[41] the Commission seeks comments regarding the method of identification of Critical Cyber Assets[42] to ensure sufficiency and accuracy. The Commission recognizes that control systems that support Bulk-Power System reliability are "only as secure as their weakest links," and that a single vulnerability opens the computer network and all other networks with which it is interconnected to potential malicious activity.[43] Accordingly, the Commission believes that any criteria adopted for the purposes of identifying a Critical Cyber Asset under CIP-002 should be based upon a Cyber Asset's connectivity and its potential to compromise the reliable operation[44] of the Bulk-Power System, rather than focusing on the operation of any specific Critical Asset(s). The Commission seeks comments on this approach.

---

[41] These include the discovery of Stuxnet, Night Dragon and RSA breaches from advanced persistent threats in July 2010, February 2011 and March 2011 respectively, where systems were compromised.

[42] In Order No. 706, the Commission declined to direct a method for identifying Critical Cyber Assets, but stated that it may revisit this circumstance in a future proceeding. *See* Order No. 706, 122 FERC ¶ 61,040 at P 284.

[43] *North American Electric Reliability Corp.*, 130 FERC ¶ 61,211, at P 15 (2010).

[44] 16 U.S.C. 824o(a)(4). The term "reliable operation" means "operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

44. Further, the Commission seeks comments on how to ensure that the directives of Order No. 706 relative to CIP-002 with respect to the concerns discussed below are addressed, resulting in a method that will lead to sufficient and accurate Critical Cyber Asset identification.

45. The Commission believes that NERC should consider the following three strategies to meet the outstanding directives and seeks comments on these strategies. First, NERC should consider applicable features of the NIST Risk Management Framework to ensure protection of all cyber systems connected to the Bulk-Power System, including establishing CIP requirements based on entity functional characteristics rather than focusing on Critical Asset size. Second, such as in the consideration of misuse, NERC should consider mechanisms for identifying Critical Cyber Assets by examining all possible communication paths between a given cyber resource and any asset supporting a reliability function. Third, NERC should provide a method for review and approval of Critical Cyber Asset lists from external sources such as the Regional Entities or NERC. Each of these strategies is discussed below.

1. NIST Framework

46. In Order No. 706, the Commission directed NERC to "monitor the development and implementation" of cybersecurity standards then being developed by the National Institute of Standards and Technology (NIST).[45] The Commission also directed NERC to

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

consider the effectiveness of the NIST standards.[46] At that time, the Commission directed NERC to address any NIST provisions that will better protect the Bulk-Power System in the Reliability Standards development process.[47] While the Commission determined not to require NERC to adopt or incorporate elements of the NIST standards, Order No. 706 left open the option of revisiting the NIST standards at a later time.[48] The Commission is not here proposing to direct that NERC use elements of the NIST standards. However, we continue to believe that the NIST framework could provide beneficial input into the NERC CIP Reliability Standards and we urge NERC to consider any such provisions that will better protect the Bulk-Power System.

47. The NIST Risk Management Framework was developed to manage the risks associated with all information systems, and offers a structured yet flexible approach that can now be applied to the electric industry. The NIST Risk Management Framework guides selection and specification of cybersecurity controls and measures necessary to protect individuals and the operations and assets of the organization, while considering effectiveness, efficiency, and constraints due to applicable laws, directives, policies, standards, or regulations. Each of the activities in the Risk Management Framework has an associated NIST security standard and/or guidance document that can be used by organizations implementing the framework. The management of risk is a key element.

---

[46] *Id.*

[47] *Id.*

[48] *Id.*

48. Two primary features of the NIST Framework are: (1) customizing protection to the mission of the cyber systems subject to protection (similar to the role identified by the NERC Functional Model); and (2) ensuring that all connected cyber systems associated with the Bulk-Power System, based on their function, receive some level of protection.[49] The Bulk-Power System could benefit from each of these tested approaches.

a. NIST Approach and the NERC Functional Model

49. The purpose of the NERC CIP Reliability Standards is to specify mandatory Requirements for responsible entities to establish, maintain, and preserve the cybersecurity of key information technology systems' assets, the use of which is essential to reliable operation of the Bulk-Power System. The CIP Reliability Standards include Requirements which are based upon the functional roles of the responsible entities as specified in the NERC Functional Model.[50] The identification of cyber systems and assets used to execute these functional roles should be the first step in identifying the systems for coverage under the CIP Reliability Standards for protection. The Functional Model should be used as a starting point when considering the applicability of the NIST Framework for securing the operation of cyber assets to provide for the Reliable Operation of the Bulk-Power System.

b. NIST Tiered Approach

50. If applied to the Bulk-Power System, the NIST Framework would specify the

---

[49] NIST SP800-53, Section 1.4, Organizational Responsibilities.

[50] Reliability Functional Model, Function Definitions and Functional Entities, Version 5, approved by NERC Board of Trustees May 2010; and, Reliability Functional Model Technical Document Version 5, approved by NERC Board of Trustees May 2010.

level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk-Power System. Cyber systems connected to the Bulk –Power System require availability, integrity, and confidentiality to effectively ensure the reliability of the Bulk-Power System.

51. The NIST Framework provides for a tiered approach to cybersecurity protection where protection of some type would be applied to all cyber assets connected to the Bulk-Power System. Under the NIST Framework, cyber assets whose compromise or loss of operability could result in a greater risk to Bulk-Power System reliability would be subject to more rigorous cybersecurity protections compared to a less important asset. The NIST Framework recognizes that all connected assets require a baseline level of protection to prevent attackers from gaining a foothold to launch further, even more devastating attacks on other critical systems.

52. Using the NIST framework, all cyber assets would also be reviewed to determine the appropriate level of cyber protection. The level of protection required for a given cyber asset is based upon its mission criticality and its innate technological risks.

2. Misuse of Control Systems

53. In Order No. 706, the Commission directed NERC to consider the misuse of control centers and control systems in the determination of Critical Assets.[51] If a perpetrator is able to misuse an asset, the attacker may navigate across and between control system data networks in order to gain access to multiple sites, which could enable

[51] Order No. 706, 122 FERC ¶ 61,040 at P 282.

a coordinated multi-site attack. Recent cybersecurity incidents[52] illustrate the importance of restricting connectivity between control systems and external networks, emphasizing the inherent risk exposure created by networking critical cyber control systems. Future mechanisms for identifying when cyber assets require protection will have to examine all possible paths between a given cyber resource and any asset supporting a reliability function.

54. In Order No. 706, the Commission expressed concerns regarding the classification of control centers and the potential misuse of control systems.[53] With regard to control centers, the Commission noted that responsible entities should be required to "examine the impact on reliability if the control centers are unavailable, due for example to power or communications failures, or denial of service attacks."[54] In addition, the Commission stated that "[r]esponsible entities should also examine the impact that misuse of those control centers could have on the electric facilities they control and what the combined impact of those electric facilities could be on the reliability of the Bulk-Power System."[55] The Commission stated that "when these matters are taken into account, it is difficult to envision a scenario in which a reliability coordinator, transmission operator or transmission owner control center or backup control center would not properly be

[52] These include the discovery of Stuxnet, Night Dragon and RSA breaches from advanced persistent threats in July 2010, February 2011 and March 2011 respectively, where systems were compromised.

[53] Order No. 706, 122 FERC ¶ 61,040 at P 280-281.

[54] *Id.* P 280.

[55] *Id.*

identified as a critical asset."[56]

55. In addition, the Commission raised concerns about the misuse of a control system that controls more than one asset.[57] Specifically, the Commission noted that multiple assets, whether multiple generating units, multiple transmission breakers, or perhaps even multiple substations, could be taken out of service simultaneously due to a failure or misuse of the control system. The Commission stated that even if one or all of the assets would not be considered as a Critical Asset on a stand alone basis, a simultaneous outage resulting from the single point of control might affect the reliability or operability of the Bulk-Power System. The Commission stated "[i]n that case, the common control system should be considered a Critical Cyber Asset."[58]

56. The Commission is concerned that the proposed CIP-002-4 bright line criteria do not adequately address the Commission's prior directive regarding the classification of control centers or take the potential misuse of control systems into account in the identification of Critical Assets. For example, the proposed bright line criteria leave a number of Critical Assets with potentially unprotected cyber assets, including a total of 222[59] control centers with no legal obligation to apply cybersecurity measures. These

[56] *Id.*

[57] *Id.* P 281.

[58] *Id.*

[59] NERC June 30, 2011 Data Response at 3.

potentially unprotected control centers involve an unknown number of associated control systems.

57. Consider the following example: Electric grid control system operation in part consists of the collection of raw data needed to run the grid, collected by a SCADA system from intelligent electronic devices (IEDs) (e.g., RTUs and synchrophasors). The SCADA data is typically aggregated by an energy management system (EMS). The EMS may, in some cases, calculate area control error (ACE) and transmit it to a balancing authority, which in turn makes computer based decisions about balancing load and generation. Those decisions are then used by the balancing authority or generation operator as part of an automated generation control (AGC) process. At each of these one or more sites, there are many data network interconnection points with other entities, (e.g., neighboring transmission operators, generation operators, and reliability coordinators) and additional connectivity to corporate data networks and elsewhere, employing several communications technologies. This results in a complex interconnection of cyber assets (including the data of those cyber assets) demanding vigilant protection.[60] These cyber systems require comprehensive protection because the interconnected system is only as strong as its weakest link.

58. Any failure to take into account the interconnectivity of control systems represents a significant reliability gap. Where modern data networking technology is used for operation of the Bulk-Power System (e.g., control systems, synchrophasors, smart grid), a

[60] *See* generally, Ron Ross, Managing Enterprise Risk in Today's World of Sophisticated Threats, National Institute of Standards and Technology (2007).

network-based cyber attack could result in multiple simultaneous outages of grid equipment and cyber systems alike through misuse of a single point of control (e.g., a SCADA control host system). Such an attack could take place by way of a cyber system associated with an asset that falls outside the CIP-002-4 bright line criteria yet is connected in common with other cyber systems on the Bulk-Power System. The risk of a cyber attack is greater now than when Order No. 706 was issued, as borne out by the recent increased frequency and sophistication of cyber attacks. It is critical, therefore, that the Commission's concerns regarding the potential misuse of control centers and associated control systems be addressed in the CIP Reliability Standards.

3. Regional Perspective

59. In Order No. 706, the Commission directed NERC to "develop a process of external review and approval of critical asset lists based on a regional perspective."[61] The Commission found that "Regional Entities must have a role in the external review to assure that there is sufficient accountability in the process [and] . . . because the Regional Entities and ERO are ultimately responsible for ensuring compliance with Reliability Standards."[62]

60. The Commission is concerned that the lack of a regional review in the identification of cyber assets might result in a reliability gap. In Order No. 706, the Commission expressed concerns regarding the need for developing a process of external

[61] Order No. 706, 122 FERC ¶ 61,040 at P 329.

[62] *Id.* P 327.

review and approval of Critical Asset lists based on a regional perspective, and that such lists are considered from a wide-area view. This process would help to identify trends in Critical Asset identification. Further, while we recognize that individual circumstances may likely vary, an external review will provide an appropriate level of consistency.[63] For example, reliability coordinators may communicate through a common system and compromise of that system could propagate across multiple regions. A cyber compromise can easily propagate across these data and control networks with potential adverse consequences to the Bulk-Power System on multi-region basis.

61. This problem may become exacerbated by any future revisions to the CIP Reliability Standards that opt to reserve a high level of independent authority to the registered entity to categorize and prioritize its cyber assets. Looking forward, it will be essential for NERC and the Regional Entities to actively review the designation of cyber assets that are subject to the CIP Reliability Standards, including those which span regions, in order to determine whether additional cyber assets should be protected.

4. Summary

62. In summary, the Commission proposes to approve NERC's proposed Version 4 CIP Standards pursuant to section 215(d)(2) of the FPA. As discussed above, it appears that the Version 4 CIP Standards represent an improvement in three respects in that they: (1) will result in the identification of certain types of Critical Assets that may not be identified under the current approach ; (2) use bright line criteria to identify Critical

[63] *Id.* P 322.

Assets, thus limiting the discretion of responsible entities when identifying Critical Assets; and (3) provide a level of consistency and clarity regarding the identification of Critical Assets.

63. While we believe that the Version 4 CIP Reliability Standards satisfy the statutory standard for approval, we also believe that more improvement is needed. As NERC explains in its Petition, the Version 4 CIP Reliability Standards are intended as "interim" and future versions will build on Version 4. We believe that the electric industry, through the NERC standards development process, should continue to develop an approach to cybersecurity that is meaningful and comprehensive to assure that the nation's electric grid is capable of withstanding a Cybersecurity Incident.[64] As discussed above, we believe that some of the essential components of such a meaningful and comprehensive approach to cybersecurity are set forth in Order No. 706.

5. Reasonable Deadline for Full Compliance with Order No. 706

64. The Commission issued Order No. 706 on January 18, 2008. In Order No. 706, the Commission approved Version 1 of the CIP Reliability Standards while also directing modifications pursuant to section 215(d)(5) of the FPA, some of which are described above. Later approved versions of the CIP Reliability Standards, and now the proposed Version 4 CIP Reliability Standards, addressed some of the directives in Order No. 706, but other directives remain unsatisfied.

[64] Section 215(a) of the FPA defines Cybersecurity Incident as "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."

65. Over three years have elapsed since the Commission issued the Final Rule in January 2008. As discussed above, we believe that it is important for the successful implementation of a comprehensive approach to cybersecurity that NERC timely addresses the modifications directed by the Commission in Order No. 706. Accordingly, the Commission proposes to set a deadline for NERC to file the next version of the CIP Reliability Standards, which NERC indicates will address all outstanding Order No. 706 directives.[65] This proposal is consistent with the views expressed in the January 2011 Audit Report of the Department of Energy's Inspector General, who found "that the Commission could have, but did not impose specific deadlines for the ERO to incorporate changes to the CIP standards."[66] Similarly, our proposal is responsive to the Audit Report finding that "the CIP standards implementation approach and schedule approved by the Commission were not adequate to ensure that systems-related risks to the Nation's power grid were mitigated or addressed in a timely manner."[67]

66. The Commission understands that, under NERC's timeline for the ongoing effort to address all outstanding Order No. 706 directives, it anticipates submitting the next version of the CIP Reliability Standards to the NERC Board of Trustees by the second quarter of 2012, and filing that version the Commission by the end of the third quarter of

[65] *See* NERC's May 27, 2011 Responses to Data Requests, Response 1 ("[t]he standard drafting team expects that the filing for the next version of the CIP Reliability Standards will address the remaining FERC Order No. 706 directives").

[66] Department of Energy Inspector General Audit Report, *Federal Energy Regulatory Commission's Monitoring of Power Grid Cybersecurity* at 6 (January 2011).

[67] *Id.* at 2.

2012.[68]

67. The Commission proposes to establish NERC's current development timeline above as a deadline for compliance with the outstanding Order No. 706 CIP Standard directives. The Commission seeks comments from NERC and other parties concerning this proposal. Further, NERC and other parties may propose and support an alternative compliance deadline.

III. Information Collection Statement

68. The Office of Management and Budget (OMB) regulations require that OMB approve certain reporting and recordkeeping requirements (collections of information) imposed by an agency.[69] The information contained here is also subject to review under section 3507(d) of the Paperwork Reduction Act of 1995.[70] We will submit this proposed rule to OMB for review.

69. As stated above, the Commission previously approved Reliability Standards similar to the proposed Reliability Standards that are the subject of the current rulemaking.[71]

---

[68] *See* NERC's May 27, 2011 Responses to Data Requests, Response 1. *See also North American Electric Reliability Corporation Reliability Standards Development Plan 2011-2013 Informational Filing Pursuant to Section 310 of the NERC Rules of Procedure*, Docket Nos. RM05-17-000, RM05-25-000, RM06-16-000 at 14 (filed April 5, 2011).

[69] 5 CFR 1320.11.

[70] 44 U.S.C. 3507(d).

[71] *North American Electric Reliability Corporation*, 130 FERC ¶ 61,271 (2010).

70. The principal differences in the information collection requirements and resulting burden imposed by the proposed Reliability Standards in this rule are triggered by the proposed changes in Reliability Standard CIP-002-4. The previous risk-based assessment methodology for identifying Critical Assets will be replaced by 17 uniform "bright line" criteria for identifying Critical Assets (in CIP-002-4, Attachment 1, "Critical Asset Criteria"). Proposed Reliability Standard CIP-002-4 would require each responsible entity to use the bright line criteria as a "checklist" to identify Critical Assets, initially and in an annual review, instead of performing the more technical and individualized risk analysis involved in complying with the currently-effective CIP Reliability Standards. As in past versions, each Responsible Entity will then identify the Critical Cyber Assets associated with its updated list of Critical Assets. If application of the bright line criteria result in the identification of new Critical Cyber Assets, such assets become subject to the remaining standards (proposed CIP-003-4, CIP-004-4, CIP-005-4a, CIP-006-4c, CIP-007-4, CIP-008-4, and CIP-009-4), and the information collection requirements contained therein.

71. We estimate that the burden associated with the annual review of the assets (by the estimated 1,501 entities) will be simplified by the "Critical Asset Criteria" in proposed Reliability Standard CIP-002-4. Rather than each entity annually reviewing and updating a Risk-Based Assessment Methodology that frequently required technical analysis and judgment decisions, the proposed bright line criteria will provide a straight forward checklist for all entities to use. Thus, we estimate that the proposal will reduce the

burden associated with the annual review, as well as provide a consistent and clear set of criteria for all entities to follow.

72. The estimated changes to burden as contained in the proposed rule in RM11-11 follow.

FERC-725B Data Collection (per proposed Version 4)	No. of Respondents[72] (1)	Average No. of Annual Responses Per Respondent (2)	Average No. of Burden Hours Per Response[73] (3)	Effect of NOPR in RM11-11, on Total Annual Hours (1)x(2)x(3)	Annual Burden Hrs. upon Implementation of RM11-11
Entities that (previously and now) will identify at least one	345 [no change]	1	1,880 [reduction of 40 hours from 1,920 to 1,880	reduction of 13,800 hours	648,600

[72] The NERC Compliance Registry as of 9/28/2010 indicated that 2,079 entities were registered for NERC's compliance program. Of these, 2,057 were identified as being U.S. entities. Staff concluded that of the 2,057 U.S. entities, approximately 1,501 were registered for at least one CIP related function. According to an April 7, 2009 memo to industry, NERC noted that only 31% of entities responding to an earlier survey reported that they had at least one Critical Asset, and only 23% reported having a Critical Cyber Asset. Staff applied the 23% (an estimate unchanged for Version 4 standards) to the 1,501 figure to estimate the number of entities that identified Critical Assets under Version 3 CIP Standards.

[73] Calculations for figures prior to applying reductions:

Respondent category b:

3 employees X (working 50%) X (40 hrs/week) X (2 weeks) = 120 hours

Respondent category c:

20 employees X (working 50%) X (40 hrs/week) X (8 weeks) = 3200 hours

20 employees X (working 20%) X (3200 hrs) = 640 hours

Total = 3840

Respondent category a:

50% of 3840 hours (category d) = 1920

Critical Cyber Asset [category a]			hours]		
Entities that (previously and now) will not identify any Critical Cyber Assets [category b]	1,144 [reduction of 12 entities from 1156 to 1,144]	1	120 [no change]	reduction of 1,440 hours [for the 12 entities]	137,280
Entities that will newly identify a Critical Asset/Critical Cyber Asset due to the requirements in RM11-11[74] [category c]	increase of 12 [formerly 0]	1	3,840[75]	increase of 46,080	46,080
Net Total	1,501 [72]			+30,840	831,960

The revisions to the cost estimates based on requirements of this proposed rule are:

- Each entity that has identified Critical Cyber Assets has a reduction of 40 hours (345 entities X 40 hrs. X @$96/hour = $1,324,800 reduction
- 12 Entities that formerly had not identified Critical Cyber Assets, but now will have them, has

[74] We estimate 12 (or 1%) of the existing entities that formerly had no identified Critical Cyber Assets will have them under the proposed Reliability Standards. This proposed rule does not affect the burden for the 6 new U.S. Entities that were estimated to newly register or otherwise become subject to the CIP Standards each year in FERC-725B, and therefore are not included in this chart.

[75] This estimated burden estimate applies only to the first three year audit cycle. In subsequent audit cycles these entities will move into category a, or be removed from the burden as an entity that no longer is registered for a CIP related function.

- a reduction of 120 hours and an increase of 3,840 hours (for a net increase of 3,720 annual hours), giving 12 entities X 3,720 hrs.@$96/hour = $4,285,440
- storage costs = 12 entities@$15.25/entity = $183

Total Net Annual Cost for the FERC-725B requirements contained in the NOPR in RM11-11= $2,960,823 ($4,285,440 +$183 -$1,324,800).

The estimated hourly rate of $96 is the average cost of legal services ($230 per hour), technical employees ($40 per hour) and administrative support ($18 per hour), based on hourly rates from the Bureau of Labor Statistics (BLS) and the 2009 Billing Rates and Practices Survey Report.[76] The $15.25 per entity for storage costs is an estimate based on the average costs to service and store 1 GB of data to demonstrate compliance with the CIP Standards.[77]

Title: Mandatory Reliability Standards, Version 4 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.

---

[76] Bureau of Labor Statistics figures were obtained from http://www.bls.gov/oes/current/naics2_22.htm, and 2009 Billing Rates figure were obtained from http://www.marylandlawyerblog.com/2009/07/average_hourly_rate_for_lawyer.html. Legal services were based on the national average billing rate (contracting out) from the above report and BLS hourly earnings (in-house personnel). It is assumed that 25% of respondents have in-house legal personnel.

[77] Based on the aggregate cost of an advanced data protection server.

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 cybersecurity 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 4 CIP Standards pursuant to section 215(d)(2) of the FPA because they represent an improvement to the currently-effective CIP Reliability Standards.

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

73. 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].

74. 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 RM11-11 and OMB Control Number 1902-0248.

IV. Environmental Analysis

75. 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.[78] 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.[79] The actions proposed here fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Certification

76. The Regulatory Flexibility Act of 1980 (RFA)[80] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities. The RFA mandates consideration of regulatory alternatives that accomplish the stated objectives of a proposed rule and that minimize any significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[81] The SBA has established a size standard for electric utilities, stating

---

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

[79] 18 CFR 380.4(a)(2)(ii).

[80] 5 U.S.C. 601-612.

[81] 13 CFR 121.101.

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.[82]

77. The Commission analyzed the affect of the proposed rule on small entities. The Commission's analysis found that the DOE's Energy Information Administration (EIA) reports that there were 3,276 electric utility companies in the United States in 2009,[83] and 3,015 of these electric utilities qualify as small entities under the Small Business Administration (SBA) definition. Of these 3,276 electric utility companies, the EIA subdivides them as follows: (1) 875 cooperatives of which 843 are small entity cooperatives; (2) 1,841 municipal utilities, of which 1,826 are small entity municipal utilities; (3) 128 political subdivisions, of which 115 are small entity political subdivisions; (4) 171 power marketers, of which 113 individually could be considered small entity power marketers;[84] (5) 200 privately owned utilities, of which 93 could be considered small entity private utilities; (6) 24 state organizations, of which 14 are small entity state organizations; and (7) 9 federal organizations of which 4 are small entity federal organizations.

78. Many of the entities that have not previously identified Critical Assets and Critical Cyber Assets are considered small entities. The new CIP version 4 bright line criteria

---

[82] 13 CFR 121.201, Sector 22, Utilities & n.1.

[83] See Energy Information Administration Database, Form EIA-861, Dept. of Energy (2009), available at http://www.eia.doe.gov/cneaf/electricity/page/eia861.html.

[84] Most of these small entity power marketers and private utilities are affiliated with others and, therefore, do not qualify as small entities under the SBA definition.

generally result in the identification of relatively larger Bulk-Power System equipment as Critical Assets. For the most part, the small entities do not own or operate these larger facilities. There is a limited possibility that these entities would have facilities that meet the bright line criteria and therefore be subject to the full CIP standards (CIP-002 through CIP-009). The Commission expects only a marginal increase in the number of small entities that will identify at least one Critical Asset under the Version 4 CIP Reliability Standards that have not done so previously.

79. The Commission estimates that only one percent (12) of the small and medium-sized entities that have not previously identified Critical Assets and Critical Cyber Assets will have an increased cost due to the proposed Reliability Standards and their identification of new Critical Cyber Assets. For each of those 12 entities, we anticipate a cost increase associated with creating a cyber security program along with the actual cyber security protections associated with the identified Critical Cyber Assets. The Commission requests comment on the potential implementation cost and subsequent cost increases that could be experienced by such small entities. Small and medium sized entities that continue to have no Critical Assets will not see any change in their burden.

80. In general, the majority of small entities are not required to comply with mandatory Reliability Standards because they are not regulated by NERC pursuant to the NERC Registry Criteria. Moreover, a small entity that is registered but does not identify critical cyber assets pursuant to CIP-002-4 will not have compliance obligations pursuant to CIP-003-4 through CIP-009-4.

81. The Commission also investigated possible alternatives. These included the Commission's adoption in Order No. 693 of the NERC definition of bulk electric system, which reduces significantly the number of small entities responsible for compliance with mandatory Reliability Standards. The Commission also noted that small entities could join a joint action agency or similar organization, which could accept responsibility for compliance with mandatory Reliability Standards on behalf of its members and also may divide the responsibility for compliance with its members.

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

VI. Comment Procedures

83. 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 that is [60] days from publication in the **FEDERAL REGISTER**]. Comments must refer to Docket No. RM11-11-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

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

in a scanned format. Commenters filing electronically do not need to make a paper filing.

85. Commenters unable to file comments electronically must mail or hand deliver an original copy of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

86. 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.

VII. Document Availability

87. 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.

88. 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.

89. User assistance is available for eLibrary and the Commission's web site during normal business hours from FERC 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.

List of subjects in 18 CFR Part 40

Electric power; Electric utilities; Reporting and record keeping requirements.

By direction of the Commission.

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Document Content(s)