128 FERC ¶ 61,291
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Marc Spitzer, and Philip D. Moeller.

North American Electric Reliability Corporation Docket No. RD09-7-000

ORDER APPROVING REVISED RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION AND REQUIRING COMPLIANCE FILING

(Issued September 30, 2009)

1. On May 22, 2009, the North American Electric Reliability Corporation (NERC) filed revised Reliability Standards for Critical Infrastructure Protection (CIP). The Commission approved eight CIP Reliability Standards in Order No. 706. In addition, pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission directed NERC to develop modifications to these CIP Reliability Standards using its Reliability Standards Development Process.[2] In its May 22, 2009 filing, NERC indicates that it is developing responsive modifications in multiple phases, and the instant filing represents the results of the first phase of the initiative.[3]

2. In this order, we approve the revised Version 2 CIP Reliability Standards under section 215(d)(2) of the FPA,[4] to become effective on April 1, 2010, as requested by NERC. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs

[1] 16 U.S.C. § 824o(d)(5) (2006).

[2] *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, *order on clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[3] *Petition of the North American Electric Reliability Corporation For Approval of Version 2 Critical Infrastructure Protection Standards*, Docket No. RD09-7-000 (May 22, 2009) (NERC Filing).

[4] 16 U.S.C. § 824o(d)(2) (2006).

NERC to develop certain modifications to the Version 2 CIP Reliability Standards, as discussed herein. We also approve NERC's proposed Version 2 Implementation Plan, subject to a compliance filing within 90 days of the date of this order, as discussed herein.

I. Background

3. On August 26, 2006, NERC in its capacity as the Electric Reliability Organization (ERO),[5] filed eight CIP Reliability Standards for approval with the Commission, to protect the Bulk-Power System from malicious or unintentional cyber events. They require Bulk-Power System users, owners, and operators to establish a risk-based assessment methodology to identify critical assets and the associated critical cyber assets essential to the critical assets' operation. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the Responsible Entities establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. The eight Reliability Standards are as follows:

> **CIP-002-1 – Cyber Security – Critical Cyber Asset Identification**: Requires a Responsible Entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.
>
> **CIP-003-1 – Cyber Security – Security Management Controls**: Requires a Responsible Entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.
>
> **CIP-004-1 – Cyber Security – Personnel & Training**: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.
>
> **CIP-005-1 – Cyber Security – Electronic Security Perimeters**: Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002-1.

[5] Section 215(e)(3) of the FPA directs the Commission to certify an ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. *Id.* § 824o(e)(3). Following a selection process, the Commission selected and certified NERC as the ERO. *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).

CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets: Requires a Responsible Entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

CIP-007-1 – Cyber Security – Systems Security Management: Requires a Responsible Entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

CIP-008-1 – Cyber Security – Incident Reporting and Response Planning: Requires a Responsible Entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

4. The Commission approved the CIP Reliability Standards in Order No. 706, finding that the proposed Standards and accompanying implementation plan are just, reasonable and in the public interest. The Commission also approved NERC's implementation plan for the Version 1 CIP Reliability Standards (Version 1 Implementation Plan).[6] However, the Commission directed NERC to develop modifications to the CIP Reliability Standards to address specific concerns raised by the Commission, including: (1) removal of the "reasonable business judgment" language from each of the Standards; (2) removal of the "acceptance of risk" exceptions from each of the Standards; (3) development of specific conditions that a Responsible Entity must satisfy to invoke the technical feasibility exception; (4) additional review and oversight regarding creation of the risk-based assessment methodology for critical cyber asset identification in CIP-002-1; and (5) revisions to certain Violation Risk Factor designations. In addition, the Commission ordered NERC to establish a timetable and work plan for developing the directed modifications to the CIP Reliability Standards.

II. NERC's Proposal

5. On May 22, 2009, NERC filed proposed modifications to the eight CIP Reliability Standards.[7] NERC stated that this filing represents the result of Phase 1 of its overall

[6] Order No. 706, 122 FERC ¶ 61,040 at P 86-90.

[7] The revised standards will be designated CIP-002-2, CIP-003-2, CIP-004-2, CIP-005-2, CIP-006-2, CIP-007-2, CIP-008-2 and CIP-009-2, with the last digit of the

(continued)

plan for revising the CIP Reliability Standards to comply with Order No. 706, and that subsequent phases will address the remainder of the Commission's directives in Order No. 706. NERC requests that, upon approval, the Version 2 CIP Reliability Standards become effective in accordance with the effective date provisions set forth in each Standard, as well as the associated implementation plan, and that upon the effective date of the Version 2 CIP Reliability Standards, the Version 1 CIP Reliability Standards be retired.[8] NERC's proposed changes to the Standards include the following:

- removal of the term "reasonable business judgment" from the purpose section of each Reliability Standard;
- removal of the term "acceptance of risk" from each Reliability Standard;
- specification in CIP-002-2 Requirement R4 that the senior manager must annually approve the risk-based assessment methodology in addition to the list of Critical Assets and Critical Cyber Assets;
- requirement in the CIP-003-2 Applicability section that all Responsible Entities must comply with CIP-003-2 Requirement R2;
- specification in CIP-003-2 Requirement R2 that a single manager with overall responsibility and authority must be designated;
- specification in CIP-003-2 Requirement R2.3 that delegations of authority must be documented;
- specification in CIP-004-2 Requirement R2 that all employees with authorized access must be trained prior to access, except in specified circumstances;
- clarification in CIP-004-2 Requirement R3 that the Responsible Entity shall have a documented personnel risk assessment program, prior to personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets;

---

standard indicating the version (Version 2 CIP Reliability Standards).

[8] Section A.5 of each of the proposed standards states: "Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after [NERC Board Of Trustees] adoption in those jurisdictions where regulatory approval is not required)." Since this order is issued by September 30, 2009, the effective date is April 1, 2010.

- clarification in CIP-006-2 Requirement R1 that the Responsible Entity shall document, implement and maintain a physical security plan, approved by the senior manager;

- identification of a Responsible Entity's compliance schedule in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

6. NERC explains that, in addition to responding to Order No. 706, the Standards Drafting Team reviewed and modified the CIP Reliability Standards to conform to the latest version of the NERC Rules of Procedure, including the Reliability Standards Development Procedure. Conformance changes are listed as administrative edits, including changes in numbering references and formats, reformatting the "Measures" sections of the Standards, and updating the "Compliance" sections. NERC also included in an appendix the stakeholder comments received in the course of balloting the proposed CIP Reliability Standards.

III. Interventions and Comments

7. Notice of the filing was published in the *Federal Register*, 74 Fed. Reg. 27,135 (2009). On June 29, 2009, Modesto Irrigation District filed a motion to intervene. FPL/NextEra Nuclear Companies and PSEG Companies both filed Out-of-Time Motions to Intervene on July 9, 2009 and August 17, 2009, respectively. American Public Power Association, Edison Electric Institute, Exelon Corporation (Exelon) and, jointly, ISO New England Inc., New York Independent System Operator, Inc. and Midwest Independent Transmission System Operator, Inc. (collectively, "the ISOs") filed motions to intervene with comments. The comments are discussed below.

8. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure,[9] the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding. The motions to intervene out-of-time by FPL/NextEra Nuclear Companies and PSEG Companies are granted, given the early stage of the proceedings, the parties' interests and the absence of undue prejudice or delay.

IV. Discussion

9. Section 215(d)(2) of the FPA[10] states that the Commission may approve, by rule or order, a proposed Reliability Standard or modification to a Reliability Standard if it

[9] 18 C.F.R. § 385.214 (2009).

[10] 16 U.S.C. § 824o(d)(2) (2006).

determines that the Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. If the Commission disapproves of the proposed Standard in whole or in part, it must remand the proposed Reliability Standard to the ERO for further consideration. Section 215(d)(5)[11] grants the Commission authority, upon its own motion or upon complaint, to order the ERO to submit to the Commission a proposed Reliability Standard or a modification to a Reliability Standard that addresses a specific matter if the Commission considers such a modified Reliability Standard appropriate to carry out section 215.

10. The Commission approves the Version 2 CIP Reliability Standards pursuant to section 215(d)(2) of the FPA. Separately, pursuant to section 215(d)(5), the Commission directs NERC to make certain modifications to the CIP Reliability Standards and the implementation plan, as discussed herein. As we found in Order No. 706, the CIP Reliability Standards provide baseline requirements for the protection of critical cyber assets that support the nation's Bulk-Power System, thus serving an important reliability goal. While the Version 2 CIP Reliability Standards respond to only a minority of the modifications directed by the Commission in Order 706, these changes are important and, when combined with the balance of the Order No. 706 directives, are expected to strengthen and improve the CIP Reliability Standards to better protect the nation's Bulk-Power System. Accordingly, we approve the CIP Version 2 Reliability Standards since they are just, reasonable, not unduly discriminatory or preferential and in the public interest. Based on the changes we approve today to the CIP Reliability Standards and other factors, the Commission may examine in a future proceeding whether changes are appropriate to the Violation Risk Factors and Violation Severity Levels for the CIP Reliability Standards.

11. We discuss below several concerns raised by commenters, as well as our own concerns regarding the proposed CIP Reliability Standards.

A. Applicability to Nuclear Power Plants

12. Exelon expresses its support for the Version 2 CIP Reliability Standards, but seeks clarification that Commission approval does not resolve the question of what NERC Standards and implementation milestones ultimately may apply to nuclear power plants. Exelon notes that this issue remains subject to the NERC stakeholder process mandated by Order No. 706-B, and explains that a stakeholder process is underway to determine an appropriate implementation timetable, which should be completed within the 180-day timetable required by Order No. 706-B. Exelon requests that the Commission clarify that approval of the Version 2 CIP Reliability Standards and the associated implementation

[11] *Id.* § 824o(d)(5).

plan should not influence the ultimate determination of an appropriate nuclear power plant implementation plan.

Commission Determination

13. The Commission clarifies that nothing in this order alters our findings in Order No. 706-B regarding the applicability of the CIP Reliability Standards, and associated implementation timetables, to facilities located at nuclear power plants.

B. Single Senior Manager Requirement

14. In Order No. 706, the Commission stated that CIP-003-1 R2 "requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards," the purpose of which "is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve."[12] In response, NERC proposes CIP-003-2 R2 as follows:[13]

> R2. Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2.
>
> . . . .
>
> R2.3 Where allowed by Standards CIP-002-2 through CIP-009-2, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

15. NERC explains that many entities expressed concern in the stakeholder process that the senior manager requirement is overly prescriptive. In response to stakeholders, NERC stated that Order No. 706's directive appropriately justifies this proposed revision because it does not dictate the management structure of the Responsible Entity. Rather, it calls for each Responsible Entity to identify a single point of accountability for the implementation and compliance with the CIP Reliability Standards.

16. NERC also noted that many entities preferred that the senior manager requirement be moved to CIP-002-2 because the applicability of CIP-003-1 can be unclear based on the steps in CIP-002-2. NERC intends to revisit the location of this requirement in a

[12] Order No. 706, 122 FERC ¶ 61,040 at P 381.

[13] For purposes of comparing versions of the Standards in this order, the underlined text indicates additions and the strike-through text indicates deletions.

future filing, but for now retains its current location on the grounds that CIP-003-2 is a governance Standard and assignment of a senior manager is a governance issue. NERC notes that it chose to clarify the applicability of CIP-003-2 Requirement R2 by adjusting the Applicability exemption language as follows:

> 4.2. The following are exempt from Standard CIP-003-2:
> . . . .
> 4.2.3 Responsible Entities that, in compliance with Standard CIP-002-2, identify that they have no Critical Cyber Assets shall only be required to comply with CIP-003-2 Requirement R2.

17. In describing the role of the single senior manager, NERC states that the Standards Drafting Team "envisions that the Senior Manager will seek the counsel of other Responsible Entity personnel in carrying out this responsibility and can delegate many of the required approvals."[14]

18. The ISOs ask the Commission to reject these changes. They argue that the mandate of a single senior manager oversteps the authority granted to NERC as the ERO in that it dictates how a Responsible Entity must comply with an objective, in this case how it establishes its management structure. As such, the ISOs assert, NERC exceeds its authority to establish standards governing the "operation" and "protection" of the Bulk-Power System. The ISOs further point to Order No. 672's distinctions of what entities need to do, as opposed to how they do it,[15] as support for their argument that this Standard seeks to regulate internal management structures without demonstrating how it will improve security. According to the ISOs, no specific mandate for a particular management structure is needed to ensure compliance.

19. The ISOs further assert that their comments on the issue are timely because the matter was not ripe for consideration until submission of proposed language by NERC. The ISOs contend that the Commission's direction to NERC in Order No. 706 was simply guidance, not a requirement that NERC revise the Reliability Standard in a particular manner. The ISOs state that there are a number of ways such an objective could be implemented. As such, the ISOs contend that this language was not previously before the Commission and comments are only now legally ripe on the issue.

---

[14] NERC Filing, Transmittal Letter at 15.

[15] ISO Comments at 6, *citing Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 260; *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

20. Finally, if the Commission accepts the single senior manager requirement, the ISOs request that it be contained within, and harmonized with, CIP-002, since CIP-002 requires a senior manager to be responsible for approving the Critical Asset and Critical Cyber Asset lists. The ISOs assert that placing the single senior manager requirement in CIP-003 creates unnecessary confusion in how to apply multiple, but similar, provisions across different Standards.

Commission Determination

21. As an initial matter, the Commission finds that consideration of the "single senior manager" language in the requirement is legally ripe. In Order No. 706, we stated our view that the CIP-003-1 Requirement R2 should be interpreted to require the designation of a single manager who has direct and comprehensive responsibility for implementation and ongoing compliance with the CIP Reliability Standards, and directed NERC to make clear the senior manager's ultimate responsibility. NERC has now proposed language effectuating this suggestion. Therefore, comments and protests to the proposal are ripe.

22. The Commission approves NERC's proposed changes to CIP-003-2. We reject the ISOs' arguments that the proposed modification dictates a Responsible Entity's internal management structure and exceeds NERC's authority to prescribe Reliability Standards. In Order No. 672, we found that in certain cases, it would be necessary for the ERO to specify "how" something is done as it may be inextricably linked to the Reliability Standard and its subsequent enforcement. In such cases, implementation features were a necessary part of a Reliability Standard if omission of such features sacrificed implementation uniformity, created uncertainty, made enforcement difficult, or complicated Commission oversight and review.[16] Accordingly, we stated we would "leave it to the ERO to develop proposed Reliability Standards that appropriately balance reliability principles and implementation features."[17]

23. Here, we find that NERC has properly balanced reliability principles and implementation features, as directed in Order No. 672, and found that the direction to appoint a single senior manager is necessary to ensure a single point of accountability for each Responsible Entity. As NERC notes, the requirement for a single senior manager does not dictate a Responsible Entity's management structure, but simply requires that there be a single point of accountability for the implementation of, and compliance with, the CIP Reliability Standards.

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

[17] *Id.*

24. We emphasize that while the single senior manager may delegate authority to perform a particular task or function, this senior manager will retain ultimate authority and accountability for implementation of, and compliance with, the CIP Reliability Standards within the organization.[18]

25. Several commenters suggest that the single manager requirement should be moved from CIP-003-1 Requirement R2 to CIP-002-1. The Commission will consider the merits of this revision once NERC proposes language to this effect.

C. Continuous Escorted Access

26. NERC proposes CIP-006-2 Requirements R1 and R1.6 as follows:

> R1. Physical Security Plan — The Responsible Entity shall ~~create~~ document, implement, and maintain a physical security plan, approved by ~~a~~ the senior manager or delegate(s) that shall address, at a minimum, the following:
> . . . .
> R1.6. ~~Procedures for~~ Continuous escorted access within the ~~physical security perimeter~~ Physical Security Perimeter of personnel not authorized for unescorted access.

27. NERC states that during the stakeholder process, entities objected to the addition of the word "continuous" to this requirement, and notes a perception on the part of stakeholders that NERC would be unable to enforce and audit compliance with this requirement. NERC explains that the Standards Drafting Team believed that the term "continuous" does not change the original intent of the requirement or the ability to audit the requirement and that, as used, "continuous" is analogous to "supervised" in that the escort is expected to be aware of the escorted visitor's actions at all times.[19] The Standards Drafting Team noted that there are numerous references available that describe how an entity's visitor control program can be verified.

28. The ISOs argue that the Commission should reject this proposed modification, clarify it or provide guidance on its meaning. They argue that demonstrating compliance with the "continuous" aspect of escorted access will be difficult, if not impossible, and it

---

[18] Order No. 706, 122 FERC ¶ 61,040 at P 295; *see also* 18 C.F.R. § 35.34(j)(3), (j)(3)(i) (2009) (explaining that an ISO or RTO must have operational control over all transmission facilities, and if it delegates any operational functions, it must demonstrate that "this sharing of operational authority will not adversely affect reliability").

[19] NERC Filing, Exh. B at 846.

is unclear what type of records or data can demonstrate that such escorting was uninterrupted. The ISOs argue that the proposed language fails to satisfy Order No. 672's direction that there should be a clear criterion or measure of whether an entity is compliant with a Reliability Standard.[20] The ISOs contend that NERC should not propose a Standard with language that has a plain meaning and then assert that, for the purposes of the Standard, the plain meaning of the relevant word is not the intent of the Standard. The ISOs note, as examples, that it is not clear if there are multiple visitors working within the Physical Security Perimeter and in the same workspace, whether each visitor requires a separate escort.

Commission Determination

29. The Commission approves Reliability Standard CIP-006-2 Requirements R1 and R1.6, as drafted as just, reasonable, not unduly discriminatory or preferential, and in the public interest, and rejects the ISOs' arguments to the contrary. The Commission finds that the term "continuous" does not alter the original intent of the Reliability Standard or NERC's ability to audit compliance with it. The Commission approves Requirement R1.6 on the basis that, as used, "continuous" is analogous to "supervised." An escort is expected to be aware of the escorted visitor's actions at all times, from the time of entry through exit. The Commission's goal is that Responsible Entities implement sound programs for visitor control and can reasonably demonstrate that they have maintained such programs. The proposed Standard helps achieve this goal and, as such, is approved.

30. Auditable visitor control programs, policies and procedures have existed for decades in both the public and private sectors as integral subsets of common and well-established industrial security programs. Common industry practices often include training requirements so that escorts understand their duties and responsibilities and employees understand what they should do if they discover unescorted visitors in areas requiring escort. Some programs even consider the sensitivity and footprint of particular facilities in determining the maximum number of visitors an escort may take charge of at any one time. Compliance with such security requirements typically includes the use and maintenance of visitor logs. Such logs can provide auditable records that identify visitors, the purpose of the visit, date and time of entry and exit, and who escorted the visitor. It is a common and well-accepted principle that when an escort takes charge of a visitor, and signs the visitor in and out of a facility, the escort is attesting that he or she has not left the visitor unattended during the entire visit. Although Reliability Standard CIP-006-2 touches on elements of a visitor control program, it does not require Responsible Entities to establish a visitor control program. Pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop a modification to Reliability

[20] ISO Comments at 9, *citing* Order No. 672, FERC Stats. & Regs. ¶ 31,204 at P 327.

Standard CIP-006-2, through the NERC Reliability Standards development process, to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit, within 90 days from the date of this order. While 90 days is a tight schedule compared to the typical development of Standards, facility security is critically important and thus justifies the accelerated deadline. NERC is also free to develop a guidance document addressing the parameters of an adequate visitor control program, if it believes such guidance is necessary.

D. Timely Updates Following Implemented Changes

31. In Order No. 706, the Commission directed NERC to revise CIP-007-1 Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented more quickly than 90 calendar days. The Commission found that 90 days is too long to allow a Responsible Entity to rely upon documentation that is not up-to-date.[21] In response, NERC proposes to modify four CIP Reliability Standards to shorten the time for updates to documents, including the Physical Security Plan in CIP-006-2, from 90 to 30 calendar days and to clarify that this time period begins upon completion of the related change. NERC notes that its proposal applies this change to all CIP Reliability Standards requiring a documentation update, not just those referenced in Order No. 706. In three of these requirements, NERC also proposes to clarify that this time period begins upon "completion" of the related change. The relevant requirements in which NERC proposes such modifications are: CIP-006-2 Requirement R1.7, CIP-007-2 Requirement R9, CIP-008-2 Requirement R1.4, and CIP-009-2 Requirement R3.

32. No comments were submitted to the Commission on this issue.

Commission Determination

33. As noted in Order No. 706, the Commission believes that 30 days provides sufficient time to update any necessary documentation, with exceptions in extraordinary circumstances, since once a modification is developed and implemented, documentation should not take significant time or resources.[22] The Commission also clarified in Order No. 706 that the time period to update documentation should begin upon final implementation of the modifications. The Commission approves NERC's proposal to reduce the documentation update timeframe from 90 days to 30 days in the four CIP

[21] *See* Order No. 706, 122 FERC ¶ 61,040 at P 651 (CIP-007-1 Requirement R9 timeline for updating documentation of changes modifying Critical Cyber Assets systems or controls); *id.* P 731 (CIP-009-1 Requirement R3 timeline to update recovery plans).

[22] *Id.* P 651-52.

Reliability Standards: (a) CIP-006-2 Requirement R1.7; (b) CIP-007-2 Requirement R9; (c) CIP-008-2 Requirement R1.4; and (d) CIP 009-2 Requirement R3.

34. The Commission also recognizes NERC's effort to address when the 30-day update period begins. NERC proposes to use the word "completion" in reference to any modification, redesign or reconfiguration prompting an update. We clarify that Responsible Entities may not seek to avoid compliance by extending completion dates significantly into the future. We recognize that project implementation may involve a lengthy timeframe, possibly with stages of the project coming online in phases. In such cases, the completion date of a significant in-service stage of the project should trigger an update within 30 days. We approve this modification with the understanding that this process will provide timely, up-to-date documentation.

E. Cyber Security Incident Response Plan

35. NERC proposes the following changes to CIP-008-2 Requirements R1 and R1.6, regarding the testing of response plans:

> **R1.** Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident ~~Response~~response plan shall address, at a minimum, the following:
>
> . . . .
>
> **R1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the ~~incident~~Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

36. During the NERC Balloting process, several industry members questioned the new sentence added to Requirement R1.6 regarding the removal of a component or system from service, some suggesting that the sentence adds confusion or might be better suited for a guidance document. The Standard Drafting Team responded that the sentence was added in accordance with Order No. 706.[23] Since the current filing responded only to the near-term directives in Order No. 706, the Standards Drafting Team suggested that the commenters resubmit their comments later in the process.

---

[23] NERC Filing, Exh. B, Record of Development of Proposed CIP Reliability Standards, Consideration of Comments on 1st Draft of CIP-002-1 through CIP-009-1 — Project 2008-0 at 108-109, *citing* Order No. 706, 122 FERC ¶ 61,040 at P 687.

37. No comments were submitted to the Commission on this issue.

Commission Determination

38. Pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop a modification to Reliability Standard CIP-008-2, Requirement R1.6, through the NERC Reliability Standards development process, to remove the last sentence of CIP-008-2 Requirement R1.6. In Order No. 706, the Commission directed NERC to "require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned."[24] We further stated that "with respect to full operational testing under CIP-008-1, such testing need not require a Responsible Entity to remove any systems from service."[25] Under Requirement R1, testing the Cyber Security Incident response plan can consist of various methods that may or may not include removing a system or component from service during testing. However, we did not see a need to modify the Reliability Standard merely to add this point and we did not direct NERC to make such a modification. Moreover, this point is not a requirement, but rather, is similar to an interpretation or clarification of a requirement.

F. Implementation Plan for Version 2 CIP Reliability Standards

39. The Commission understands that NERC's filing includes two independent documents relating to implementation of the Version 2 CIP Reliability Standards. The first is labeled "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," is located at pages 813 – 814 of the filing submitted in this proceeding. The second, labeled as "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards," is located at pages 817 – 824 of the filing. The Commission will consider each in turn below.

Commission Determination

40. We reject the first document identified above, "Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2," because it is unnecessary and causes confusion. For instance, this document discusses the proposed effective date of the Version 2 CIP Reliability Standards, but this discussion is unnecessary because each such Standard includes a provision describing its effective date. The first document also discusses the date by which "newly registered entities" must comply with the Version 2 CIP Reliability Standards. This document does not define "newly registered

[24] Order No. 706, 122 FERC ¶ 61,040 at P 686.

[25] *Id.* P 687.

entities," but its statements appear consistent with the timeline for compliance set forth in Table 3 of the second document that applies to "Entities Registering in 2008 and Thereafter." We believe the first document is confusing since it is unclear how it relates to the second document. If NERC believes that information contained in this document is useful for explanatory purposes, NERC should incorporate the relevant information into the second implementation plan to create a single, comprehensive document.

41. Considered alone, we find that the second document identified above, "Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards," (the Version 2 Implementation Plan or Version 2 plan) lacks clarity and could be open to multiple interpretations on some topics. Commission Staff prepared a document reflecting our concerns in this regard, which is attached to this order. We direct NERC to submit, within 90 days of the date of issuance of this order, a compliance filing that includes a revised Version 2 Implementation Plan, addressing the Version 2 CIP Reliability Standards, that clarifies the matters specified in the attachment to this order.

G. Next Phases of Modifications

42. NERC states that the Standards Drafting Team adopted a multi-phased strategy to revise the CIP Reliability Standards due to the extensive scope of the project. According to NERC, this filing represents Phase 1 of that project and directives not addressed in this filing will be included in later phases.[26] In the first phase, NERC states that it focused on timely, administrative and conforming modifications, including removal of the "reasonable business judgment" and "acceptance of risk" language before July 1, 2009.

43. In Order No. 706, we directed NERC to develop a timetable as well as submit a work plan for developing and filing for approval the modifications directed by the Commission to the CIP Reliability Standards.[27] While we do not object to NERC's multi-phased approach, NERC should provide more information regarding the status of these modifications, such as the inclusion of lessons learned,[28] the clarification that

[26] NERC Filing, Transmittal Letter at 7-8.

[27] Order No. 706, 122 FERC ¶ 61,040 at P 13, 89.

[28] *Id.* P 686.

Responsible Entities cannot except themselves from the CIP Reliability Standards,[29] and identification of the core training elements and parameters for exceptional circumstances.[30]

44. We direct NERC to submit as part of the compliance filing required by this order an update of the timetable that reflects the plan to address remaining Commission directives from Order No. 706. The filing should be a report of current status, addressing all of the projects including those that are underway and already planned as well as those that have been deferred or not yet scheduled, with a summary description of which Order No. 706 directives NERC plans to address during each phase.

The Commission orders:

(A) NERC's revised Version 2 CIP Reliability Standards are hereby accepted for filing, as discussed in the body of this order.

(B) NERC is hereby required to submit compliance filings within 90 days from the date of this order, as discussed in the body of this order.

(C) The Commission hereby directs NERC to develop modifications to the CIP Reliability Standards using its Reliability Standards Development Process within 90 days of the date of this order, as discussed in the body of this order.

By the Commission. Commissioner Kelly is not participating.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[29] *Id.* P 90.

[30] *Id.* P 431, 443.

ATTACHMENT

Compliance Issues On Implementation Plan

a. The Version 2 Implementation Plan states at page 1 that it identifies the schedule for becoming compliant with the requirements of CIP-003-2 through CIP-009-2 and their successor Standards "for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed." The use of the phrase "existing Implementation Plan" here and elsewhere on page 1 of the Version 2 Implementation Plan causes confusion as to whether the Version 1 Implementation Plan or the proposed plan is being referenced. We direct NERC to clarify that the "existing" implementation plan is the Version 1 Implementation Plan.

b. The Version 2 Implementation Plan refers at page 3 several times to "this New Asset Implementation Plan." We direct NERC to delete or change this inaccurate reference.

c. The Version 2 Implementation Plan refers at pages 3 and 4 several times to "an established CIP Compliance program as required by an existing Implementation Schedule." We direct NERC to clarify the meaning of "an established CIP Compliance program." In particular, we direct NERC to state whether a "CIP Compliance program" includes a program for complying with CIP-002 or is limited to a CIP compliance program for CIP-003 through CIP-009, as stated for Category 1 listed under the heading "Implementation Schedule" on page 1 of the Version 2 Implementation Plan. We also direct NERC to clarify the meaning of "an existing Implementation Schedule."

d. We direct NERC to clarify whether the Version 2 Implementation Plan contemplates that the Version 1 Implementation Plan will be retired upon the effective date of the Version 2 CIP Reliability Standards. If not, we require further explanation as to how the Version 1 Implementation Plan will still be applicable. The revised plan should be clear which entities must continue to rely upon the Version 1 Implementation Plan, and to what extent in which circumstances.

e. In the third paragraph of page 1, the Version 2 Implementation Plan refers to "some requirements" for which a Responsible Entity is expected to be Compliant upon the designation of the newly identified Critical Cyber Asset, stating that these instances are "annotated as '0'." We observe that the Version 2 Implementation Plan does not annotate any requirement as "0." We direct NERC to explain or delete this statement and to list each requirement for which a Responsible Entity is expected to be Compliant immediately upon designation of a newly identified Critical Cyber Asset.

f. In the third paragraph of page 1, the Version 2 Implementation Plan also refers to "other requirements" for which the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date, stating that these are annotated as "existing." We observe that Table 2 of the Version 2 Implementation Plan annotates the following requirements as "existing" for "Milestone Category 2": CIP-003-2, R1 through R3 and CIP-004-2 Requirement R1. We direct NERC to confirm whether these requirements are the only requirements annotated as "existing" in the Version 2 Implementation Plan and, if not, to list each other requirement for which the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date.

g. At page 1, under the heading "Implementation Schedule," the Version 2 Implementation Plan lists three categories. Category 2 refers to "An existing Cyber Asset becomes subject to CIP Reliability Standards, *not due to planned change*," while Category 3 refers to "A new or existing Cyber Asset becomes subject to CIP Reliability Standards *due to planned change*" (emphasis in original). We direct NERC to clarify, for purposes of these categories, the meaning of the statement "Cyber Asset becomes subject to CIP Standards." We note that pursuant to CIP-002-2 Requirement R3, a Responsible Entity must consider which of its Cyber Assets are Critical Cyber Assets essential to the operation of a Critical Asset. In that sense, all of a Responsible Entity's Cyber Assets become subject to CIP Reliability Standards when the entity undertakes to comply with CIP-002-2 Requirement R3. We also observe that at page 2, the Version 2 Implementation Plan states that the term "Cyber Asset becomes subject to the CIP standards" applies to "all Critical Cyber Assets, as well as to other (non-critical) Cyber Assets within an Electronic Security Perimeter." However, this statement does not make clear whether NERC intends that formula to be the definition of the term. We direct NERC to clarify the meaning of the term "planned change" that appears in the description of both categories, because the Version 2 Implementation Plan does not define that term.

h. At page 3, the Version 2 Implementation Plan states that Category 2 applies "only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement" (emphasis in original). We direct NERC to clarify this statement because of our concern that it provides an unintended incentive for Responsible Entities to delay identification of assets that trigger the implementation timelines set forth in Table 2. For example, in January 2010 a Responsible Entity could obtain information indicating that an asset already in service should be identified as a Critical Cyber Asset. However, if the Responsible Entity does not so "identify" the asset until December 2010, the period the Version 2 Implementation Plan allows for becoming compliant would begin as much as 11 months later than if the Responsible Entity identified the asset as a Critical Cyber Asset immediately after obtaining information indicating that the asset should be so identified. We note that CIP-002-

2 Requirement R3 states that a Responsible Entity shall review its list of Critical Cyber Assets "at least annually, and update it as necessary."

i. Also at page 3, with respect to a business merger where all parties have identified Critical Cyber Assets and have "existing but different" CIP compliance plans in place, the Version 2 Implementation Plan provides that the merged Responsible Entity has one calendar year from the merger's effective date to determine either to combine the programs or operate them separately under a common Senior Manager. The Version 2 Implementation Plan further states that at the conclusion of the calendar year, the merged Responsible Entity will use the Category 2 milestones to consolidate the separate programs. We direct NERC to specify the minimum extent of difference between the compliance plans that would trigger this provision of the Version 2 plan, because, absent this specificity, any difference between the compliance plans could activate this provision. We further direct NERC to explain whether this provision would extend the time period for compliance with applicable Version 2 requirements for the merged Responsible Entity if it (a) did not identify any additional Critical Cyber Assets after the effective date of the merger; or (b) did identify such additional assets.

j. At the last paragraph of page 4, the Version 2 plan states, "Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards." The Commission observes that the third sentence is not accurate if the phrase "these standards" is interpreted to include CIP-002-2. We direct NERC to revise this sentence to clarify its meaning.

k. We direct NERC to clarify whether the abbreviations used in Table 3 of the Version 2 Implementation Plan (BW, SC, C and AC) have the same meaning as the counterpart abbreviations in the Version 1 plan.

l. We observe generally that further clarification on the treatment of mergers and acquisitions at pages 3 and 4 of the Version 2 Implementation Plan is appropriate and perhaps could be achieved with explanatory text and examples in an introductory section. The Commission believes that it would be helpful to entities and promote uniform understanding if introductory explanations and/or diagrams were to address the following merger-specific instances: (1) a merger of two or more entities where none have identified a Critical Cyber Asset; (2) a merger of two or more entities where one has identified at least one Critical Cyber Asset; and (3) a merger of two or more entities where each has identified at least one Critical Cyber Asset.

m. We also observe that one or more existing Responsible Entities that have identified at least one Critical Cyber Asset could form a new entity that heretofore has not been registered on the NERC Compliance Registry. Upon the new entity's registration, it could be argued that Table 3 of the Version 2 Implementation Plan would apply to it because it would be an entity "registering in 2008 and thereafter." Interpreted literally, Table 3 then would exempt the newly registered entity from compliance with CIP-003-2 Requirement R2 for 12 months after registration and with the remainder of the requirements of the Version 2 CIP Reliability Standards for 24 months after registration. We direct NERC to explain how it would address this situation in the context of Version 2 implementation. More broadly, because innumerable permutations of merger and acquisition scenarios exist, we direct NERC to incorporate into the Version 2 Implementation Plan explicit language to preclude unfair delay of compliance due to the structure of particular transactions.

Document Content(s)