

130 FERC ¶ 61,271
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

North American Electric Reliability Corporation

Docket No. RD09-7-002

ORDER ON COMPLIANCE

(Issued March 31, 2010)

1. On December 29, 2009, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted a compliance filing in response to the Commission's September 30, 2009 order.¹ The filing includes (1) submission of a full set of "Version 3" Critical Infrastructure Protection (CIP) Reliability Standards CIP-002-3 through CIP-009-3 that include modifications to two CIP Reliability Standards, (2) a revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, (3) an Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 (Version 3 CIP Implementation Plan), and (4) an updated timetable that reflects NERC's plan to address the Commission directives set forth in Order No. 706.² In this order, we approve the modified CIP Reliability Standards, with an effective date of October 1, 2010. Further, we approve the revised Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. However, we reject the Version 3 CIP Implementation Plan, as discussed below.

¹ *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (September 30 Order), *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009).

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

I. Background

2. In Order No. 706, the Commission approved the “Version 1” CIP Reliability Standards, determining that the proposed Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission further approved NERC’s Implementation Plan for the Version 1 CIP Reliability Standards. In addition, the Commission directed NERC to develop modifications to the CIP Reliability Standards to address specific concerns raised by the Commission and establish a timetable and work plan for developing the modifications.

3. On May 22, 2009, NERC filed eight “Version 2” CIP Reliability Standards, which proposed certain modifications in response to the Commission’s directives set forth in Order No. 706. NERC stated that the Version 2 filing represented the result of Phase 1 of its overall 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 also submitted two implementation plans: (1) Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2 and (2) Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards.

4. In the September 30 Order, the Commission approved the Version 2 CIP Reliability Standards and directed the ERO to make certain modifications to the CIP Reliability Standards and the implementation plans within 90 days from the date of the order. The Commission directed the ERO to develop a modification to Reliability Standard CIP-006-2 to add a requirement on visitor control programs, including the use of visitor logs to document entry and exit.³ The Commission also directed the ERO to develop a modification to Reliability Standard CIP-008-2, Requirement R1.6 to delete language regarding the need to remove systems from service during full operational testing. Further, the Commission found that the “Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards” lacked clarity and directed NERC to submit a revised plan that clarifies certain matters.⁴ The Commission rejected the “Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2,” because it was confusing and duplicative of other documents. Finally, the Commission directed NERC to submit an update of the timetable to address the remaining Commission directives from Order No. 706.

³ September 30 Order, 128 FERC ¶ 61,291 at P 29-30.

⁴ *Id.*, P 41 and Attachment.

II. NERC Filing

5. On December 29, 2010, NERC submitted a compliance filing in response to the September 30 Order. NERC explained that, while the filing proposes modifications to two CIP Reliability Standards, NERC submitted the full set of CIP Reliability Standards, CIP-002-3 through CIP-009-3, as the Version 3 CIP Reliability Standards for ease of reference and to simplify applicable entities' understanding of the appropriate implementation dates.

6. NERC modified Reliability Standard CIP-006, Requirement R1.6 to include provisions for a visitor control program:

R1.6 A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

NERC also modified Reliability Standard CIP-008-3 to remove the last sentence of Requirement R1.6, as directed by the September 30 Order.

7. NERC further proposed two implementation plans. First, NERC submitted an Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities, revised to address the concerns and clarifications set forth in the Attachment to the September 30 Order. Second, NERC submitted an Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3 (Version 3 CIP Implementation Plan), which states that prior versions of the CIP Reliability Standards will be retired when the Version 3 CIP Reliability Standards become effective. It also states that the original Version 1 Implementation Plan "is in practice retired" as of December 31, 2010.

8. In response to the Commission's directive, NERC included an updated timeline regarding its plans to comply with the remaining Order No. 706 directives. While not required by the September 30 Order, NERC also filed conforming changes to Violation

Risk Factors and Violation Severity Levels to accommodate revisions made by the proposed Version 3 CIP Reliability Standards.⁵

III. Notice and Responsive Pleadings

9. Notice of the filing was published in the *Federal Register*, 75 Fed. Reg. 1766 (2010), with interventions and protests due on or before January 19, 2010. Edison Electric Institute and American Public Power Association filed timely motions to intervene.

IV. Discussion

A. Procedural Matters

10. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2009), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

B. Version 3 CIP Reliability Standards

11. Section 215(d)(2) of the Federal Power Act (FPA) authorizes the Commission to approve, by rule or order, a proposed Reliability Standard or modification to a Reliability Standard if it determines that the Standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest.⁶

12. As discussed above, the September 30 Order directed modifications to the CIP Reliability Standards to address two issues. The Version 3 CIP Reliability Standards adequately address our concerns. In particular, the modification of Reliability Standard CIP-006, Requirement R1.6 to include a visitor control program is a significant improvement to the CIP Reliability Standards. This provision makes explicit that applicable entities must document the entry and exit of visitors. Further, NERC's removal of certain language from CIP-008 provides needed clarity to the Reliability Standard. Generally, as the Commission 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.⁷

⁵ The Commission does not address the Version 3 Violation Risk Factors and Violation Severity Levels submitted with this filing in this order, and will address these at a later time.

⁶ 16 U.S.C. § 824o(d)(2) (2006).

⁷ Order No. 706, 122 FERC ¶ 61,040 at P 24.

Accordingly, pursuant to section 215(d)(2) of the FPA, we approve the Version 3 CIP Reliability Standards as just, reasonable, not unduly discriminatory or preferential and in the public interest. The effective date for the Version 3 CIP Reliability Standards shall be October 1, 2010.⁸

C. Implementation Plan Documents

1. Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

13. In the September 30 Order, the Commission expressed concern that the “Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards” lacked clarity and could be open to multiple interpretations on some topics. The Commission directed the ERO to revise the Implementation Plan and address 13 issues identified in an attachment to the September 30 Order.

14. On compliance, NERC submitted a revised plan with a clarified title: “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities,” responding to the Commission’s concerns. NERC explains that this document applies to both Version 2 and Version 3 CIP Reliability Standards (i.e., CIP-002-2 through CIP-009-2 and CIP-002-3 through CIP-009-3). NERC requests that the Commission approve this Implementation Plan, with an effective date of April 1, 2010 to coincide with the effective date of the Version 2 CIP Reliability Standards.

15. We find that NERC’s revised plan adequately addresses the clarity concerns set forth in the September 30 Order. Accordingly, the Commission approves the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities,” to become effective April 1, 2010.

2. Version 3 CIP Implementation Plan

16. In the September 30 Order, the Commission rejected the “Implementation Plan for Version 2 of Cyber Security Standards CIP-002-2 through CIP-009-2,” finding that it was unnecessary, since each Reliability Standard includes an effective date provision, and confusing, in part because it was unclear how it related to the companion implementation

⁸ Each of the Version 3 CIP Reliability Standards specifies the following as its effective date: “The first day of the third calendar quarter after applicable regulatory approvals have been received...” Since this order is issued on or before March 31, 2010, the Version 3 CIP Reliability Standards will become effective in the United States on October 1, 2010.

plan referenced above.⁹ The Commission noted that the information contained in the document was useful for explanatory purposes and advised NERC to incorporate the relevant information into the companion plan entitled “Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards” to create a single, comprehensive document.

17. In its Compliance Filing, NERC presented a brief history of the CIP implementation plans, explaining that the Version 1 Implementation Plan provided compliance milestones across four timetables. Responsible entities were classified as Table 1, Table 2, Table 3, or Table 4 entities, depending on which functions they were registered for, whether they previously had been required to certify compliance with Urgent Action Cyber Standard 1200, and the date of their registration. NERC stated that all entities were to reach the “auditably compliant” milestone by December 31, 2010. NERC noted that the Version 2 Implementation Plan, rejected by the Commission, contained the statement that when the Version 2 CIP Reliability Standards became effective, the Version 1 CIP Reliability Standards and the Version 1 Implementation Plan would be retired.

18. In response to the Commission’s concerns, NERC presents a revised document, the Version 3 CIP Implementation Plan. NERC asserts that this document makes five statements: (1) prior versions of the CIP Reliability Standards will be retired when the Version 3 CIP Reliability Standards become effective; (2) responsible entities must be compliant with Version 3 CIP Reliability Standards on the date those standards become effective; (3) the Version 3 CIP Reliability Standards become effective on the first day of the third quarter following regulatory approval; (4) Newly Identified Critical Cyber Assets and Newly Registered Entities are covered by the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities”; and (5) the original implementation plan for the Version 1 CIP Reliability Standards will, as a practical matter, end on December 31, 2010, because on that date all Table 1, 2, and 3 entities must be auditably compliant.

19. NERC states that it intends for two implementation plans to be in effect as of April 1, 2010: the Version 3 CIP Implementation Plan “which effectively implements the FERC-approved Version 1 implementation plan dates for Table 1, Table 2, and Table 3 entities for Version 1, Version 2, or Version 3 standards, whichever are in effect; as well as the Implementation Plan for Newly Identified Critical Cyber Assets and Newly

⁹ September 30 Order at P 40.

Registered Entities.” NERC further asserts that after December 31, 2010, when the Version 1 Implementation Plan dates are retired, only the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities will remain in effect.

Commission Determination

20. The Commission rejects the Version 3 CIP Implementation Plan. We understand that NERC intends this Version 3 CIP Implementation Plan to serve as a guide to which CIP Reliability Standards and which implementation plans are in effect at a given time. We find this document unnecessary and confusing, primarily because the Version 3 CIP Implementation Plan is presented as an actionable plan rather than an informational guide. However, the Implementation Plan itself does not determine the effective date, or retirement, of the CIP Reliability Standards. Rather, the functions listed in the document occur as a result of the Commission’s approval of the Reliability Standards themselves.

21. To provide clarity regarding the effective dates of the CIP Reliability Standards and implementation plans, as well as which entities must be compliant at which time, we provide the following information based on Commission orders to date:

- All responsible entities that registered by March 31, 2008, must become compliant with the CIP Reliability Standards according to the milestones stated in the Version 1 Implementation Plan.¹⁰
- All responsible entities that registered on or after April 1, 2008, must become compliant with the CIP Reliability Standards according to the milestones stated in the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” approved by this order.
- If a responsible entity subsequently identifies a new Critical Cyber Asset, after reaching the “Compliant” milestone for CIP-002 under the applicable Implementation Plan based on its registration date, the responsible entity shall either bring the newly identified Critical Cyber Asset into compliance immediately upon identification or according to the milestones enumerated in the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” approved by this order.
- The Version 1 Implementation Plan is fully retired for all subject entities as of March 31, 2011, for three reasons: (1) Table 1, Table 2, and Table 3 entities under the Version 1 Implementation Plan are scheduled to reach the “Auditably Compliant”

¹⁰ Order No. 706, 122 FERC ¶ 61,040 at P 86; *see also infra* n.11.

phase by December 31, 2010; (2) the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” replaces Table 4 of the Version 1 Implementation Plan for any entities that registered on or after April 1, 2008; and (3) an entity registered on the last possible date to be subject to the Version 1 Implementation Plan must reach the “Auditably Compliant” phase by March 31, 2011.¹¹

- The Version 2 CIP Reliability Standards shall be effective as of April 1, 2010 based on the effective date formula contained in each of the standard.¹²
- The Version 3 CIP Reliability Standards shall be effective as of October 1, 2010 according to the effective date formula contained in each of the standards.
- The two documents filed by NERC on May 22, 2009 to comprise a Version 2 Implementation Plan are not in effect for any entity at any time.

D. Compliance Timetable

22. Pursuant to the Commission’s directives in the September 30 Order, NERC submitted a timetable regarding its plan to comply with the remaining Order No. 706 directives. We accept this timetable as complying with the Commission’s informational request.

The Commission orders:

(A) The Version 3 CIP Reliability Standards are hereby accepted, as discussed in the body of this order.

(B) The Version 3 CIP Implementation Plan is hereby rejected, as discussed in the body of this order.

¹¹ We note that NERC refers to the Version 1 Implementation Plan as expiring on December 31, 2010 when, in fact, March 31, 2011 is the last possible date an entity subject to the Version 1 Implementation Plan should reach the final Table 4 milestones. The Version 1 Implementation Plan has been effectively extended because NERC changed the date of the applicability of the Table 3 milestones in the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” approved by this order. In the version filed by NERC on May 22, 2009, Table 3 was applicable to entities registering “in 2008 and thereafter” rather than “in April 2008 or thereafter” as the version approved today states.

¹² September 30 Order at P 5 n.8.

(C) The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities is hereby accepted, as discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.