129 FERC ¶ 61,236
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

North American Electric Reliability Corporation Docket No. RD09-7-001

ORDER DENYING REHEARING AND GRANTING CLARIFICATION

(Issued December 17, 2009)

1. On October 30, 2009, the Edison Electric Institute (EEI), on behalf of its member companies, submitted a request for rehearing or, in the alternative, a motion for clarification and extension of time of the Commission's September 30, 2009 Order[1] approving the revised Version 2 Critical Infrastructure Protection (CIP) Reliability Standards, in the above mentioned docket. For the reasons discussed below, we deny the request for rehearing, but grant the motion for clarification and request for an extension of time.

I. Background

2. On August 26, 2006, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), filed eight CIP Reliability Standards for approval with the Commission. These CIP Reliability Standards require certain users, owners, and operators of the Bulk-Power System to comply with specific requirements to safeguard critical cyber assets. Pursuant to the CIP Reliability Standards, Bulk-Power System users, owners, and operators must 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.

[1] *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (2009) (September 30 Order).

3. The Commission approved the CIP Reliability Standards in Order No. 706, finding that the proposed Standards and accompanying implementation plan are just, reasonable, not unduly discriminatory or preferential, and in the public interest.[2] The Commission approved NERC's implementation plan for the Version 1 CIP Reliability Standards.[3] In addition, 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 CIP Reliability Standards; (2) removal of the "acceptance of risk" exception from the CIP Reliability 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. The Commission also ordered NERC to establish a timetable and work plan for developing the modifications to the CIP Reliability Standards directed in Order No. 706.

4. On May 22, 2009, NERC filed proposed modifications to the eight CIP Reliability Standards. NERC stated that this 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's proposed changes included the following: (1) removal of the term "reasonable business judgment" from the purpose section of each Reliability Standard; (2) removal of the term "acceptance of risk" from the Standards; (3) 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; (4) requirement in the CIP-003-2 Applicability section that all Responsible Entities must comply with CIP-003-2 Requirement R2; (5) specification in CIP-003-2 Requirement R2 that a single manager with overall responsibility and authority must be designated; (6) specification in CIP-003-2 Requirement R2.3 that delegations of authority must be documented; (7) specification in CIP-004-2 Requirement R2 that all employees with authorized access must be trained prior to access, except in specified circumstances; (8) 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; (9) clarification

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

in CIP-006-2 Requirement R1 that the Responsible Entity shall document, implement and maintain a physical security plan, approved by the senior manager; and (10) identification of a responsible entity's compliance schedule in the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.

5. In the September 30 Order, the Commission approved the Version 2 CIP Reliability Standards pursuant to section 215(d)(2) of the Federal Power Act (FPA).[4] Separately, pursuant to section 215(d)(5),[5] the Commission directed NERC to make certain modifications to the CIP Reliability Standards and the implementation plan within 90 days from the date of the order. First, the Commission directed the ERO to develop a modification to Reliability 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. Second, the Commission directed the ERO to develop a modification to Reliability Standard CIP-008-2, Requirement R1.6, through the NERC Reliability Standards development process, to remove from CIP-008-2 Requirement R1.6 the last sentence which addresses the need to remove systems from service during full operational testing. Third, the Commission directed NERC to submit a revised Version 2 Implementation Plan that clarifies certain matters of concern to the Commission. Fourth, the Commission directed NERC to submit an update of the timetable that reflects the plan to address the remaining Commission directives from Order No. 706.

6. On October 30, 2009, EEI filed a request for rehearing or, in the alternative, a motion for clarification and extension of time of the September 30 Order. EEI raises two issues: (1) whether the Commission erred in directing the ERO to develop a visitor access program within 90 days; and (2) whether the Commission erred in directing the specific changes to Requirement R1.6 of Reliability Standard CIP-008-2, rather than requesting that the NERC Reliability Standards development process consider modifications to the requirement.

II. Discussion

A. The Requirement to Develop a Visitor Control Program

7. EEI states that while the Commission directs the ERO through the 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

[4] 16 U.S.C. § 824o(d)(2) (2006).

[5] *Id.* § 824o(d)(5).

of this order,"[6] the order is not clear as to what the Commission is requiring in terms of the nature and extent of the programs to be developed. EEI argues that this directive lacks clarity and provides an unreasonably short period of time in which to complete the required NERC Standards development process, and therefore seeks rehearing of this requirement.

8. In the event that the Commission does not grant rehearing, EEI requests that the Commission clarify the parameters of such programs so that the NERC Reliability Standards development process will have a clear direction for its activities in response to this directive. Specifically, EEI states that the Commission should clarify whether it is only requesting that registered entities maintain visitor logs. EEI requests that the Commission also clarify that a requirement for visitor control programs is limited to personnel without authorization for unescorted access and not for personnel with authorization for unescorted access. EEI further requests that the Commission clarify what it meant by the term "visitor" and what the requested visitor control program should encompass.

9. EEI also contends that the requirement to complete the modification within 90 days is unrealistically short given the uncertain nature of the task, as well as the fact that all responsible entities have physical security plans, which EEI understands to include procedures for visitor control, as obligated under CIP-006-2, Requirement R1. EEI argues that the September 30 Order does not explain why the 90-day deadline is appropriate, particularly when it is highly likely that a requirement on visitor controls is already a part of physical security plans. EEI also moves for an extension of time for the NERC Reliability Standards development process to develop the requested requirement on visitor control programs, for an additional 90 days after the Commission issues the requested clarification or, as an alternative, that the Commission direct NERC to develop "procedures" or "guidelines" or "best practices" for physical security plans.

Commission Determination

10. We deny EEI's requests for rehearing, but grant the motion for clarification on this issue, and an extension of time to develop the requirement. The September 30 Order 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."[7] The Commission was clear in its request that the modification must require a visitor control program and include documentation of entry and exit. While the

[6] EEI Request for Rehearing at 5, *citing* September 30 Order, 128 FERC ¶ 61,291 at P 30.

[7] September 30 Order, 128 FERC ¶ 61,291 at P 30.

Commission provided sufficient guidance to the ERO as to how it should modify the Reliability Standard, we will grant a 90-day extension from the date of issuance of this order so that the ERO will have ample time to develop the requested requirement on visitor control programs.

11. The Commission in the September 30 Order provided clear direction as well as examples of several common elements that constitute sound and auditable visitor control programs.[8] Physical security plans deal primarily with three classes or categories of individuals: 1) unauthorized personnel; 2) authorized personnel who have been granted unescorted access privileges; and 3) authorized personnel who require escort. The first category pertains to trespassers and others on the premises without permission. The second category relates to personnel that have been granted unescorted access privileges based on successful completion of their particular host's requisite training and background checks. This group typically includes permanent employees and certain vendors or contractors requiring frequent or long-term physical access to sensitive areas. The third category encompasses all other types of personnel, commonly referred to as "visitors."

12. For purposes of the Commission's directive pertaining to CIP-006-2, visitor control programs are intended to address safety and physical security issues associated with visitors only. Visitors are generally authorized invitees or licensees whose presence the Responsible Entity has deemed necessary or legitimate to its enterprise, but have not been explicitly granted unescorted access privileges. "Visitor" designations are typically assigned to personnel requiring infrequent or short-term physical access to sensitive areas; or to those who will eventually be granted unescorted access, but who have not yet completed the requisite training and vetting processes. Examples include vendors, contractors or maintenance staff or services, audit and assessment teams, new employees, etc. By virtue of their class, visitors require greater scrutiny, including continuous escort, and logs recording locations visited and dates and times of entry and exit as previously enumerated in the September 30 Order.

B. Reliability Standard CIP-008-2, Cybersecurity Incident Response Plan

13. Reliability Standard CIP-008-2 Requirement R1.6, as revised, provides:

> **R1.6.** Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the 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

[8] *Id.*

> does not require removing a component or system from service during the test.

In the September 30 Order, the Commission directed the Standards Development Team to remove the last sentence of Requirement R1.6.[9]

14. EEI requests that the Commission clarify its position regarding this deletion. EEI agrees with the Commission's statement that "the sentence could be inferred by Requirement 1 and Requirement 1.6," however, EEI argues that the sentence does not harm the Requirement in any way by remaining part of the Standard. Further, EEI asserts that the Commission acknowledged that the sentence "is similar to an interpretation," and that all interpretations have to be approved through the Reliability Standards development process and accepted by the Commission. EEI contends that the sentence provides additional clarity to the Requirements and does not harm reliability, and therefore, should not be removed from the Reliability Standard. EEI also states that the Commission determined in Order No. 706 that "such testing need not require a Responsible Entity to remove any systems from service,"[10] and if the Commission determines that the sentence should still be deleted, the Commission should provide clarification whether the sentence departs in any way from its statement in Order No. 706.

15. EEI further contends that this directive to make specific changes to Requirement R1.6 contravenes the Commission's prior orders on the Standards development process, as set forth in Order Nos. 693, 693-A[11] and 706, and therefore requests rehearing. EEI argues that in those orders, the Commission made clear that it "do[es] not wish that a direction for modification be so overly prescriptive as to preclude the consideration of viable alternatives in the ERO's Reliability Standards process."[12] EEI asserts that in ordering the specific language changes to Requirement R1.6, the Commission has directed an "exclusive" outcome to address its concerns, contrary to Order No. 693.[13] Instead, EEI states that the Commission should provide an understanding of its concerns,

---

[9] *Id.* P 38.

[10] Order No. 706, 122 FERC ¶ 61,040 at P 687.

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

[12] Order No. 693-A, 120 FERC ¶ 61,053 at P 40.

[13] *Id., citing* Order No. 693, FERC Stats & Regs. ¶ 31,242 at P 185.

and direct the Reliability Standards development process to present an outcome that addresses its concerns.

Commission Determination

16. As stated above, Order No. 706 does state 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,"[14] and the Commission does not assert that the sentence included in Requirement 1.6 departs from this principle. As stated in the September 30 Order, 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. However, similar to industry members that questioned the addition of the new sentence to Requirement R1.6 during the NERC balloting process, the Commission believes the new sentence is unnecessary and is better suited for a guidance document. Further, the Commission reiterates that it did not direct NERC to make such a modification and does not see a need to modify the Reliability Standard merely to add this point.

17. The Commission is not prescribing this specific change as an exclusive solution to its concerns regarding Requirement R1.6. As we have stated in previous orders, the ERO can propose an alternative solution that it believes is equally effective and efficient to eliminate confusion.[15]

The Commission orders:

(A) The request for rehearing is hereby denied, as discussed in the body of this order.

(B) EEI's motion for clarification and request for an extension of time of 90 days from the issuance of this order are hereby granted.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.

[14] Order No. 706, 122 FERC ¶ 61,040 at P 687.

[15] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 186.

Document Content(s)