130 FERC ¶ 61,184
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. RD10-3-000

ORDER APPROVING RELIABILITY STANDARD INTERPRETATION

(Issued March 18, 2010)

1. Pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission approves the interpretation of the North American Electric Reliability Corporation (NERC), of the Commission-approved Critical Infrastructure Protection (CIP) Reliability Standard, CIP-007-2—Systems Security Management, Requirement R2.

## I. Background

### A. EPAct 2005 and Mandatory Reliability Standards

2. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, which are subject to Commission review and approval. Specifically, the Commission may 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.[2] Once approved, the Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[3]

[1] 16 U.S.C. § 824o (2006).

[2] *Id.* § 824o(d)(2).

[3] *Id.* § 824o(e)(3).

3. Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO[4] and, subsequently, certified NERC as the ERO.[5] On January 18, 2008, the Commission issued a Final Rule, Order No. 706, approving eight CIP Reliability Standards, including CIP-007-1.[6] In addition, pursuant to section 215(d)(5) of the FPA, the Commission directed NERC to develop certain modifications to the CIP Reliability Standards to address certain concerns.[7] Subsequently, the Commission approved modifications to the CIP Reliability Standards, including CIP-007-2.[8]

4. NERC's Rules of Procedure provide that a person that is "directly and materially affected" by Bulk-Power System reliability may request an interpretation of a Reliability Standard.[9] In response to such a request, the ERO assembles a team with relevant expertise to address the requested interpretation and forms a ballot pool. NERC's Rules provide that, within 45 days, the team will draft an interpretation of the Reliability Standard and submit it to the ballot pool. If approved, the interpretation is appended to the Reliability Standard and filed with the applicable regulatory authority for regulatory approval.

### B. Reliability Standard CIP-007

5. Reliability Standard CIP-007-2 addresses the system security management practices of applicable entities. The Reliability Standard requires applicable entities to

---

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

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

[6] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *order on reh'g*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009).

[7] 16 U.S.C. § 824o(d)(5).

[8] *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (2009). The modified, version 2, CIP Reliability Standards take effect on April 1, 2010.

[9] NERC Rules of Procedure, Appendix 3A, Reliability Standards Development Procedure, Version 6.1, at 26-27 (2007).

define methods, processes, and procedures for securing critical cyber assets and non-critical cyber assets located within an electronic security perimeter. Requirement R2 of the Reliability Standard pertains to ports and services necessary for normal and emergency operations. Specifically, Requirement R2 provides:

> R.2 The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> R2.1 The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
>
> R2.2 The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> R2.3 In the case where unused ports and services cannot be disabled due to technical limitations,[10] the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

## II. NERC Petition

6. On November 17, 2009, NERC submitted a petition (NERC Petition) seeking Commission approval of an interpretation of CIP-007-2, Requirement R2.[11] In the petition, NERC explains that the Western Electricity Coordinating Council (WECC) requested that NERC interpret whether the term "port," as used in the phrase "ports and

[10] We note that the Commission has stated that the "due to technical limitations" language in R2.3 must be read to treat any such technical limitation as a technical feasibility exception that must be analyzed using the technical feasibility exception process. Order No. 706, 122 FERC ¶ 61,040 at P 589, 597.

[11] NERC states that when it received the request for interpretation submitted by WECC in March 2009, CIP-007-1 (version 1) was the Commission-approved version of that reliability standard in effect. Accordingly, NERC processed the request pursuant to CIP-007-1. As previously noted, the Commission has since approved version 2 of CIP-007-2, which will go into effect on April 1, 2010. NERC explains that its interpretation applies equally to Reliability Standard, CIP-007-2, version 2. *See* NERC Petition at 1 n.4. The Commission concurs with NERC that it is appropriate to append the interpretation, approved herein, to CIP-007-2, rather than CIP-007-1.

services," means a physical (hardware) or a logical (software) connection to a computer, or both.

7. Consistent with the NERC Rules of Procedure, NERC assembled a team to respond to the request for interpretation and presented the proposed interpretation to industry balloting, similar to the Reliability Standards development process. NERC states that stakeholders approved the interpretation using this process and that the NERC Board of Trustees approved the resulting interpretation in November 2009.

8. NERC's interpretation of Reliability Standard CIP-007-2, Requirement R2, states that the term "ports," used as part of the phrase "ports and services," refers to logical ports only, e.g., Transmission Control Protocol (TCP) ports where interface with communication services occurs.[12] Thus, CIP-007-2, Requirement R2, is not applicable to physical ports. NERC explains that its interpretation comports with the language in the Reliability Standard and supports the "reliability objective of ensuring that [only] those ports and services required for normal and emergency operations are enabled."[13]

9. NERC states that the inclusion of physical ports was not the intention of CIP-007. Nonetheless, NERC recognizes that increased protections would be possible by addressing the security of physical ports but that such an effort would need to be vetted through its Reliability Standards Development Procedure and made clear in the requirement language of a future updated standard. NERC indicates that consideration of including both physical and logical ports in the requirements of the Reliability Standard is already within the scope of its project to comply with Order No. 706, which is targeted for completion by the end of 2010.[14]

## III. Notices of Filings and Responsive Pleadings

10. Notice of the NERC Petition was published in the *Federal Register*, with interventions and protests due on or before December 8, 2009.[15] Edison Electric Institute, American Municipal Power, and Exelon Corporation filed timely motions to intervene.

---

[12] *See* NERC Petition at 8-9.

[13] *Id.* at 9.

[14] *Id.* Further, NERC references a Board of Trustees resolution recommending promptly addressing any gaps or deficiencies, in a Reliability Standard, which are identified during the interpretation process.

[15] 74 Fed. Reg. 64064 (2009).

## IV. Discussion

### A. Procedural Matters

11. 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. Commission Determination

12. We approve NERC's interpretation of Requirement R2 of Reliability Standard CIP-007-2, as discussed below.

13. We agree that NERC's interpretation represents the language in the Reliability Standard as it is currently worded. However, like NERC, we are concerned that neither CIP-007-2 in particular, nor the CIP Reliability Standards in general, adequately address technical opportunities to mitigate risks associated with unused *physical* ports. The practice of disabling or otherwise securing unused physical ports is a basic and integral component of sound defense-in-depth cyber security practices, yet it is absent from the current Reliability Standards. The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010.[16] Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports. The term "ports and services" is a well-established term of art that refers to logical ports only. Thus, to avoid potential continued confusion and commingling of common and well-established terms of art, the Commission strongly encourages NERC to approach the security of physical ports as a separate provision, apart from the existing logical "ports and services" language, so that the clarity established by this interpretation remains intact.

[16] *See* NERC Petition at 5-6 (Project 2008-06 – Cyber Security – Order 706).

The Commission orders:

NERC's interpretation of Requirement R2 of Reliability Standard CIP-007-2 is hereby approved, effective as of the date of this order, as discussed in this order.

By the Commission.

( S E A L )

Kimberly D. Bose,
Secretary.