

132 FERC ¶ 61,051
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

North American Electric Reliability Corporation

Docket No. RD10-13-000

ORDER APPROVING RELIABILITY STANDARD INTERPRETATION

(Issued July 15, 2010)

1. Pursuant to section 215 of the Federal Power Act (FPA),¹ the Commission approves the North American Electric Reliability Corporation's (NERC) interpretation of the Commission-approved Critical Infrastructure Protection (CIP) Reliability Standard, CIP-006-2, Cyber Security – Physical Security of Critical Cyber Assets, Requirement R1.1.

I. Background

A. EPAAct 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 Standard may be enforced in the United States 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 ERO⁴ 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-006-1.⁶ 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-006-2⁸ and CIP-006-3.⁹ Requirement R1.1 of CIP-006 is identical in version 2 and version 3.

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.¹⁰ 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 approval.

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) (approving version 2 of the CIP Reliability Standards effective April 1, 2010).

⁹ *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010) (approving version 3 of the CIP Reliability Standards to take effect on October 1, 2010).

¹⁰ NERC Rules of Procedure, Appendix 3A, Reliability Standards Development Procedure, Version 7, at 30 (2010).

B. Reliability Standard CIP-006-2

5. Reliability Standard CIP-006-2 addresses physical security of critical cyber assets. This Reliability Standard ensures applicable entities implement a physical security program for the protection of critical cyber assets. CIP-006-2, Requirement R1 requires entities to document, implement, and maintain a physical security plan. Sub-requirements R1.1 through R1.8 set out the minimum requirements for a physical security plan. Requirement R1.1, the subject of this proceeding, provides:

R1.1 All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

II. NERC Petition

6. On April 20, 2010, NERC submitted a petition (NERC Petition) seeking Commission approval of an interpretation of CIP-006-2, Requirement R1.1.¹¹ The interpretation arises from PacifiCorp’s request that NERC clarify whether alternative measures to control physical access to cyber assets must be physical in nature. PacifiCorp further asked, if such alternative measures must be physical in nature, whether the physical barrier must prevent physical access, e.g., concrete encased fiber, or if alternative measures that effectively mitigate risks associated with physical access qualify, e.g., cameras, motion sensors, or encryption.

7. NERC’s interpretation of Reliability Standard CIP-006-2, Requirement R1.1 clarifies that alternative measures to “control” physical access may comprise both physical as well as logical measures. Specifically, NERC states the alternative measures may be physical or logical, as long as the alternative measure provides security equivalent or better to a completely enclosed (“six-wall”) border. The interpretation further clarifies that alternative measures may include, but are not limited to (i) multiple physical access control layers within a non-public, controlled space and (ii) logical control measures such as data encryption and/or circuit monitoring to detect unauthorized

¹¹ NERC states that when it received PacifiCorp’s request for interpretation in February 2009, CIP-006-1 (version 1) was the Commission-approved version of that reliability standard in effect. Accordingly, NERC processed the interpretation request referencing CIP-006-1. The Commission since has approved version 2 (CIP-006-2), which went into effect April 1, 2010, and version 3 (CIP-006-3), which will become effective on October 1, 2010. NERC explains that the interpretation is equally relevant to all three versions of Requirement R1.1 of CIP-006. *See* NERC Petition at 1, n.4.

access or physical tampering.¹² NERC concludes that the main objective of the Reliability Standard can be achieved through any measure, physical or logical, that succeeds in controlling physical access to the critical cyber asset with an equivalent security posture.¹³

8. NERC states that this interpretation was presented for industry balloting and was approved by the ballot pool. NERC's Board of Trustees subsequently approved the interpretation on February 6, 2010.¹⁴

III. Notice and Responsive Pleadings

9. Notice of NERC's Petition was published in the *Federal Register*, with interventions and protests due on or before May 12, 2010.¹⁵ ISO New England Inc., American Municipal Power, Inc., and Exelon Corporation filed timely motions to intervene. No comments or protests were filed.

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 (2010), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

B. Commission Determination

1. NERC's Interpretation

11. We approve NERC's interpretation of Requirement R1.1 of Reliability Standard CIP-006-2.¹⁶ We agree that NERC's interpretation is consistent with the language in Requirement R1.1 of CIP-006-2.

¹² NERC Petition at 6.

¹³ *Id.* at 6-7.

¹⁴ *Id.* at 4.

¹⁵ 75 Fed. Reg. 23,750 (2010).

¹⁶ As NERC noted in its petition, version 2 of the CIP Standards is the FERC-approved version currently in effect. Thus the version of CIP-006 that includes the FERC-approved interpretation of Requirement R1.1 will be referred to as CIP-006-2c.

2. Reliability Standard CIP-006-2

12. Critical cyber assets are defined in NERC's Glossary of Terms as programmable electronic devices and communication networks including hardware, software, and data essential to the reliable operation of critical assets.¹⁷ Reliability Standard CIP-006-2 deals primarily with physical protection of equipment. However, as defined, data itself can also be a critical cyber asset, and there may be circumstances where physical protection measures are insufficient to protect that data. In such cases, logical measures, such as encryption, may be necessary to protect that data. The nature of the particular critical cyber asset must be considered in each case to determine what physical and/or logical measures are necessary to achieve and maintain in each case the three cyber security protection tenets of confidentiality, integrity, and availability.¹⁸

13. NERC should, when proposing modifications to its CIP Reliability Standards, distinguish between physical and logical protective measures in a manner that more clearly aligns such measures with the particular security objectives it is trying to achieve. Further, if a responsible entity is unable to strictly comply with CIP-006-2, the responsible entity would submit a technical feasibility exception request that proposes an alternative solution utilizing an appropriate combination of physical and logical protection measures that ensures the protection of all cyber assets (both equipment and data) in a manner that achieves an equivalent or better level of security as strict compliance with CIP-006-2.¹⁹

However, once version 3 of the CIP standards take effect on October 1, 2010, the version of CIP-006 that includes the interpretation of R1.1 approved in this order will be referred to as CIP-006-3c.

¹⁷ See *Glossary of Terms Used in NERC Reliability Standards*, updated April 20, 2010 (available online at http://www.nerc.com/docs/standards/rs/Glossary_of_Terms_2010April20.pdf) (defining "Critical Cyber Assets" and "Cyber Assets").

¹⁸ Often referred to by the acronym CIA, confidentiality, integrity and availability are the three primary tenets of information and cyber security. See, e.g., International Standards Organization's International Standard ISO/IEC 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*, at § 3.2.3 (available online at <http://www.iso27001security.com/html/27000.html>) ("Information security includes three main dimensions: confidentiality, availability and integrity.").

¹⁹ Any "alternative measure" proposed to comply with CIP-006-2 is subject to the technical feasibility exception (TFE) procedures as directed by the Commission in its
(continued...)

The Commission orders:

NERC's interpretation of Requirement R1.1 of Reliability Standard CIP-006-2 is hereby approved, effective as of the date of this order.

By the Commission. Commissioner LaFleur voting present.

(S E A L)

Kimberly D. Bose,
Secretary

January 21, 2010 Order Approving TFE Procedures. *See North American Electric Reliability Corp.*, 130 FERC ¶ 61,050, at P 20 (2010); *see also North American Electric Reliability Corp.*, Compliance Filing in Response to January 21, 2010 Commission Order Concerning Appendix 4D, at 4, Docket No. RR10-1-001 (April 21, 2010) (revising section 1.3 of the TFE Procedure to include CIP-006-2, Requirement R1.1 in the list of Applicable Requirements as well as a reference to the interpretation that is the subject of this order).

Document Content(s)

RD10-13-000.DOC.....1-6