135 FERC ¶ 61,167
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. RD10-8-000

ORDER APPROVING INTERPRETATION OF RELIABILITY STANDARD AND ESTABLISHING TECHNICAL CONFERENCE

(Issued May 19, 2011)

1. On December 22, 2009, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), petitioned the Commission to approve an interpretation of two provisions of Critical Infrastructure Protection (CIP) Reliability Standard CIP-006-2 (Cyber Security – Physical Security of Critical Cyber Assets).[1] We approve NERC's interpretation, which will become effective from the date of this order.

2. Additionally, we direct the Commission's staff to convene a technical conference to address issues raised in this order.

I. Background

3. On January 18, 2008, pursuant to section 215(d)(2) of the Federal Power Act (FPA),[2] the Commission issued Order No. 706 approving eight CIP Reliability Standards

[1] South Carolina Electric & Gas and the U.S. Army Corps of Engineers sought interpretation of version 1 of CIP-006 (CIP-006-1) on August 9, 2007 and September 12, 2008, respectively, and the interpretation approved by NERC is based on CIP-006-1. NERC requests approval of the interpretation with respect to version 2 of CIP-006 (CIP-006-2), however, because version 2 was in effect at the time the petition was filed. The Commission subsequently approved version 3 of CIP-006 (CIP-006-3), which became effective on October 1, 2010. The Commission concludes that NERC's interpretation is relevant to all three versions of the CIP-006 Reliability Standard. Accordingly, the Commission's determination is binding on the current version of the Reliability Standard, CIP-006-3.

[2] 16 U.S.C. § 824o(d)(2) (2006).

proposed by NERC, including CIP-006-1.[3] In addition, pursuant to section 215(d)(5) of the FPA,[4] the Commission directed NERC to develop certain modifications to the CIP Reliability Standards to address certain concerns. Subsequently, the Commission approved modifications to the CIP Reliability Standards, including CIP-006-2[5] and CIP-006-3.[6] Requirements R1.1 and R4 of CIP-006 are identical in versions 2 and 3.

4. NERC's Rules of Procedure provide that all persons "directly and materially affected" by Bulk-Power System reliability may request an interpretation of a Reliability Standard.[7] In response to a request, NERC assembles a team with relevant expertise to address the requested interpretation and forms an industry ballot pool. NERC's Rules of Procedure provide that, within 45 days, the team will draft an interpretation of the Reliability Standard, with subsequent balloting. If approved by industry ballot and the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed with the applicable regulatory authority for approval. When the subject Reliability Standard is next revised, the interpretation is incorporated into the Reliability Standard.

II. NERC Filing

5. In its petition, NERC proposes an interpretation of Requirements R1.1 and R4 of CIP-006. NERC interprets Requirement R1.1 to exempt dial-up accessible devices using non-routable protocols from the scope of that Requirement. NERC maintains that its interpretation is justified by the exemption found in Section D.1.5.2 of CIP-006-2.[8]

---

[3] *See 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).

[4] 16 U.S.C. § 824o(d)(5) (2006).

[5] *North American Electric Reliability Corp.*, 128 FERC ¶ 61,291 (2009).

[6] *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010).

[7] NERC Rules of Procedure, Appendix 3A, Reliability Standards Development Procedure, Version 6.1, at 26-27 (2007). As noted below, NERC operated under Version 6.1 of the Reliability Standards Development Procedure when it developed this interpretation.

[8] In CIP-006-1, the exemption language is found in Section D.1.4.4. In this order, we employ the numbering scheme found in CIP-006-2, -3, which places the exemption language in Section D.1.5.2. Accordingly, we cite to Section D.1.5.2 when referring to the exemption language.

NERC interprets Requirement R4: (1) as requiring monitoring and logging of access only for ingress into a physical security perimeter; and (2) as defining "time of access" to mean the "the time an authorized individual enters the physical security perimeter."[9]

6. Consistent with NERC's Rules of Procedure, a NERC-assembled ballot body, consisting of industry stakeholders, developed the interpretation using the NERC Reliability Standards Development Procedure, Version 6.1, and the NERC Board of Trustees approved the interpretation.[10] The interpretation does not modify the language contained in the Requirements under review. NERC requests that the Commission approve the interpretation, effective immediately after approval, consistent with the Commission's procedures.

III. Procedural Matters

7. Notice of NERC's filing was published in the *Federal Register*, 75 Fed. Reg. 354-55 (2010), with interventions and protests due on or before January 21, 2010. No motion to intervene or protest was received.

IV. Discussion

8. The Commission approves NERC's proposed interpretation of Requirements R1.1 and R4, as discussed below. The ERO's interpretation is consistent with the existing exemption language of the CIP-006 Reliability Standard. In addition, we direct the Commission's staff to convene a technical conference to address the issues raised below regarding the cybersecurity implications of exempting dial-up accessible devices using non-routable protocols from Requirement R1.1 of CIP-006 and to discuss whether any modifications to the Reliability Standard are necessary.

A. Requirement R1.1

9. Requirement R1.1 of CIP-006-2 addresses processes that a responsible entity must include in its physical security plan to ensure that all cyber assets within an electronic security perimeter also reside within an identified physical security perimeter. The specific language of Requirement R1.1 is:

> All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed

[9] NERC Filing at 13.

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

> ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.

10. Section D.1.5.2 (Additional Compliance Information) of CIP-006-2 provides:

> For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006 for that single access point at the dial-up device.

1. NERC Interpretation

11. NERC interprets Requirement R1.1 as follows:

> Dial-up assets are Critical Cyber Assets, assuming they meet the criteria in CIP-002-[2], and they must reside within an Electronic Security Perimeter. However, physical security control over a critical cyber asset is not required if that asset does not have a routable protocol. Since there is minimal risk of compromising other critical cyber assets dial-up devices such as Remote Terminals Units that do not use routable protocols are not required to be enclosed within a "six-wall" border . . .
>
> CIP-006-[2] – Additional Compliance Information [D.1.5.2] identifies dial-up accessible assets that use non-routable protocols as a special class of cyber assets that are not subject to the Physical Security Perimeter requirement of this standard.[11]

12. NERC provides the following rationale to support its interpretation: (1) Section D.1.5.2 explicitly exempts dial-up accessible devices using non-routable protocols from Requirement R1.1; (2) the CIP drafters intended to limit Requirement R1.1 through the exemption language in Section D.1.5.2; and (3) NERC's stakeholders approved Requirement R1.1 based on the understanding that Section D.1.5.2 exempts dial-up accessible devices using non-routable protocols from Requirement R1.1.

13. NERC maintains that the proposed interpretation supports the reliability goals of the Reliability Standard by providing clarity and certainty and ensuring the implementation of a physical security program for the protection of critical cyber assets. While not a rationale for approval, NERC asserts that dial-up accessible devices using non-routable protocols pose a "minimal risk" to the Bulk-Power System, though NERC does not provide support for that statement in its petition.

---

[11] *Id*. at 7.

2. Commission Determination

14. We approve NERC's interpretation of Requirement R1.1 of CIP-006-2. NERC's interpretation is consistent with the exemption language found in Section D.1.5.2 of the Reliability Standard.

15. Requirement R1.1 is an all-inclusive requirement, providing that all critical cyber assets must reside within a physical security perimeter. NERC's interpretation, therefore, depends on reading the exemption language found in Section D.1.5.2 into Requirement R1.1 itself. We conclude that, applying principles of interpretation, it is appropriate to exempt dial-up accessible devices using non-routable protocols from the scope of Requirement R1.1 based on the language found in Section D.1.5.2.

16. In Order No. 693, we addressed the significance of compliance-related provisions contained in a Reliability Standard, as follows:

> The Commission adopts the position it took in the Notice of Proposed Rulemaking (NOPR) that, while Measures and Levels of Non-Compliance provide useful guidance to the industry, compliance will in all cases be measured by determining whether a party met or failed to meet the Requirement given the specific facts and circumstances of its use, ownership or operation of the Bulk-Power System. As we explained in the NOPR, and reiterate here:
>
> > The most critical element of a Reliability Standard is the Requirements. As NERC explains, "the Requirements within a standard define what an entity must do to be compliant . . . [and] binds an entity to certain obligations of performance under section 215 of the FPA." If properly drafted, a Reliability Standard may be enforced in the absence of specified Measures or Levels of Non-Compliance.[12]

17. NERC states that the original drafting team developed CIP-006-1 before learning from the Commission in Order No. 693 that Requirements define the compliance obligations, instead believing that information in other sections could be used to construe the meaning of the Requirements.[13] NERC suggests that had it known the Commission's view when it drafted CIP-006-1, it would have placed the exemption in the Requirement

---

[12] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, at P 253, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007).

[13] NERC Filing at 8.

itself rather than in the "Additional Compliance Information" section. NERC also represents that it intends to bring the Reliability Standard into compliance with Order No. 693 by moving the exemption language into Requirement R1.1 as part of its on-going CIP revision process.[14]

18. The Commission affirms the holding in Order No. 693 that Requirements are the most critical elements of a Reliability Standard, and that they "define what an entity must do to be compliant." Nevertheless, we are persuaded that Requirement R1.1 was originally drafted and approved by NERC with the intent that dial-up accessible devices using non-routable protocols would be exempted pursuant to Section D.1.5.2. Moreover, the Requirement was drafted and approved prior to issuance of Order No. 693.

19. Based on the foregoing, the Commission approves NERC's interpretation of Requirement R1.1 in CIP-006-2.

20. In the filing, NERC characterizes the risks posed to the Bulk-Power System by exempting dial-up devices using non-routable protocols from Requirement R1.1 as "minimal."[15] As mentioned above, this is not a rationale for approval of the interpretation. However, NERC does not provide support for its assessment. We are concerned that the exempted devices could be targeted as a means for compromising the Bulk-Power System. The possibility of a significant risk or increased level of risk over time arising from the approved interpretation warrants further study of the issue. Our concern is echoed in the filing where NERC states that it "will further consider the issue and impacts identified in this request to determine if improvements are necessary to the requirements to enhance protection of the Bulk Power System."[16] In that respect, we believe that a staff-led technical conference is a useful vehicle for collecting and discussing relevant data from NERC, subject matter experts, and industry to confirm or allay our concerns. The technical conference should, at a minimum, address questions such as the number of devices that are implicated by the approved interpretation, the level of risk to the Bulk-Power System, and the impact of mitigating any risks.

---

[14] "[I]nformed at this point by substantial Commission guidance provided since NERC was certified to be the ERO and since the CIP-006-1 standard was originally drafted, NERC fully recognizes the need to revise the language of Requirement R1.1 itself to explicitly identify the exception noted in Section D.1.4.4. NERC commits to doing so as it considers the revision of the CIP family standards in response to the Commission's Order No. 706." *Id.* at 8-9.

[15] *Id.* at 7.

[16] *Id.* at 9.

21. Accordingly, we direct the Commission's staff to convene a technical conference to examine the cybersecurity implications of the exemption and whether updating it is appropriate to reflect the Commission's understanding of the risks associated with dial-up accessible assets that use non-routable protocols.

B. Requirement R4

22. Requirement R4 of CIP-006-2 specifies controls for managing physical access to a physical security perimeter. Requirement R4 addresses the need to record sufficient information to uniquely identify individuals entering a physical security perimeter and their time of access twenty-four hours a day, seven days a week. To that end, Requirement R4 requires implementation of one or more methods of managing physical access (i.e., card keys, special locks, security personnel, or other authentication devices).

1. NERC Interpretation

23. NERC's interpretation of Requirement R4 clarifies: (1) that the monitoring and logging of access to a physical security perimeter is presently limited to ingress; and (2) that the term "time of access" refers to "the time an authorized individual enters the physical security perimeter."[17] NERC maintains that this interpretation directly supports the reliability purpose of the Reliability Standard because it provides clarity and certainty to the requirement that "time of access" be recorded.

2. Commission Determination

24. The Commission approves NERC's proposed interpretation of Requirement R4 of CIP-006-2. NERC's interpretation is consistent with and adds clarity to the CIP-006-2 Reliability Standard.

The Commission orders:

(A) NERC's interpretation of Requirements R1.1 and R4 of Reliability Standard CIP-006-2 is hereby approved, effective as of the date of this order, as discussed in the body of this order.

[17] *Id.* at 13.

(B) The Commission's staff is directed to convene a technical conference, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.