142 FERC ¶ 61,203
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

North American Electric Reliability Corporation Docket No. RD12-3-000

ORDER REMANDING PROPOSED INTERPRETATION
OF RELIABILITY STANDARD CIP-006-4

(Issued March 21, 2013)

1. On May 23, 2012, the North American Electric Reliability Corporation (NERC) submitted a petition requesting approval of an interpretation to Requirement R1.1 of Reliability Standard CIP-006-4. Pursuant to section 215(d)(4) of the Federal Power Act (FPA), we remand the proposed interpretation.[1] As discussed below, the Commission finds that the proposed definition of a communication network underlying the interpretation is not a reasonable definition. In addition, the Commission finds that the proposed interpretation is inconsistent with the existing Commission-approved interpretation of Requirement R1.1. Accordingly, we remand NERC's proposed interpretation as unjust, unreasonable, unduly discriminatory and preferential, and not in the public interest.

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 provide for the reliable operation of the Bulk-Power System, subject to Commission review and approval.[2] On February 3, 2006, the Commission issued Order No. 672 to

[1] 16 U.S.C. § 824o(d)(4) (2006).

[2] *Id.* § 824o(d)(2).

implement the requirements of section 215 of the FPA governing electric reliability.[3] In July 2006, the Commission certified NERC as the ERO.[4]

3. 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.[5] In response, the ERO will assemble a team with relevant expertise to address the requested interpretation and also form a ballot pool. NERC's Rules of Procedure provide that, within 45 days, the team will draft an interpretation of the Reliability Standard and submit it to the ballot pool. If approved by the ballot pool and subsequently by the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed with the applicable regulatory authorities for approval.

B. NERC Petition

4. In its May 23, 2012 Petition, NERC requests Commission approval of a proposed interpretation of Requirement R1.1 of Reliability Standard CIP-006-4. The stated purpose of the Reliability Standard is to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.[6]

---

[3] *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).

[4] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *order on compliance*, 118 FERC ¶ 61,030, *order on clarification and reh'g*, 119 FERC ¶ 61,046 (2007), *aff'd sub nom. Alcoa Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[5] NERC Rules of Procedure, Appendix 3A, Standard Processes Manual, at 27-29 (January 31, 2012).

[6] NERC defines Cyber Assets as "[p]rogrammable electronic devices and communication networks including hardware, software, and data." *NERC Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary), at 4. NERC defines Critical Cyber Assets as "Cyber Assets essential to the reliable operation of Critical Assets." *Id.* In turn, Critical Assets are defined as "[f]acilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System." *Id.* Section 215(a)(8) of the FPA defines "cybersecurity incident" as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those *programmable electronic devices and*

(continued…)

5. Requirement R1.1 states:

> 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.

6. In the Petition, NERC explains that it received a request from Progress Energy seeking an interpretation of Requirement R1.1 of CIP-006-1.[7] Specifically, Progress Energy presented the following issue for interpretation:

> It is unclear from the stated [CIP] requirements the extent [Electronic Security Perimeter] wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the [Electronic Security Perimeter].

7. The NERC interpretation drafting team developed the following response:

> CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset." The definition of "Cyber Asset" in the NERC Glossary of Terms Used in Reliability Standards includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

---

communications networks including hardware, software and data that are essential to the reliable operation of the bulk power system." 16 U.S.C. 824o(a)(8) (emphasis added).

[7] At the time the request for interpretation was submitted to NERC, Version 1 of the CIP Reliability Standards was in effect. Subsequent modifications to the CIP Reliability Standards in Versions 2, 3, and 4 are not material to the substance of the interpretation request. *See* Petition at 1.

> This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (*e.g.*, wiring), which makes it distinct from the interpretation in CIP-006-3c, appendix 1. The interpretation in CIP-006-3c, appendix 1, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).

8. In the Petition, NERC states that the proposed interpretation is consistent with the stated purpose of the Reliability Standard, which is to ensure that Critical Cyber Assets are protected. NERC summarizes the drafting team's conclusion by stating that "the interpretation discusses the distinction between a Cyber Asset and the underlying components of Cyber Assets that are not themselves classified Cyber Assets. Since the requirement only applies to a Cyber Asset, and wiring is not a Cyber Asset, the requirement does not apply to wiring."[8]

9. With regard to wiring, NERC explains that the interpretation drafting team determined that the Commission-approved definition of Cyber Asset in the *Glossary of Terms Used in NERC Reliability Standards* "does not include communication mediums (i.e., wiring)."[9] NERC states that a "communication network, which is included in the definition of a Cyber Asset, is typically a set of devices and a population of data, but not the wires or any other supporting component."[10] In addition, NERC states that although data is included in the definition of Cyber Asset, the act of transmitting data over a wire in and of itself does not automatically transform wiring into a Cyber Asset.

10. Finally, in support of the drafting team's conclusion that wiring is not a Cyber Asset, NERC states that "[a]ssuming *arguendo* that 'wiring' is a Cyber Asset, wiring would then be subject to all Reliability Standards that apply to Cyber Assets."[11] NERC states that this would lead to "an unintended application of the CIP standards and the wasting of limited industry resources."[12]

---

[8] Petition at 8.

[9] *Id.*

[10] *Id.* at 9.

[11] *Id.* at 9.

[12] *Id.*

II. Notices of Filing and Responsive Pleadings

11. Notice of NERC's petition was published in the *Federal Register*, 77 Fed. Reg. 33,207 (2012), with interventions and protests due on or before June 13, 2012. No interventions or protests were filed.

III. Commission Determination

12. We remand NERC's proposed interpretation of Reliability Standard CIP-006-4, Requirement R1.1. As explained below, we find that the proposed definition of a communication network underlying the interpretation is not a reasonable definition. We also find that the proposed interpretation is inconsistent with the existing Commission-approved interpretation of Requirement R1.1.

A. Communication Networks

13. In the Petition, NERC states that a communication network is "typically a set of devices and a population of data, but not the wires or any other supporting component."[13] NERC does not provide any support for this reading of the term other than stating that "the interpretation drafting team determined that the definition of Cyber Asset in the *Glossary of Terms Used in NERC Reliability Standards* does not include communication mediums (i.e., wires)."[14] The Commission finds that this proposed definition is at odds with the general understanding of communication networks. A communication network cannot function without communication mediums. For many communication networks, the communication mediums will include network cables (i.e., wires). Thus, it does not appear reasonable to conclude that, for the purposes of the CIP Reliability Standards, a communication network does not include wires or other communication mediums.

14. We note that available definitions of "network" do not support the interpretation drafting team's conclusion. Specifically, a "network" is defined as "a system of computers, peripherals, terminals, and databases *connected by communication lines*"[15] or,

---

[13] *Id.*

[14] *Id.* at 8.

[15] Network. 2013. in *Merriam-Webster.com*. Retrieved February 20, 2013, from www.merriam-webster.com/dictionary/network (emphasis added). *See also* Network. 2013. in *thefreedictionary.com*. Retrieved February 20, 2013, from www.thefreedictionary.com/network (A group or system of electric components and connecting circuitry designed to function in a specific manner).

more simply, as "a series of points interconnected by communication channels."[16] Likewise, existing non-NERC standards addressing information and cyber security also address both power and communication wiring.[17] In light of the general understanding of communication networks, we cannot accept NERC's inadequately supported explanation.

15. As noted above, NERC argues that wires are not subject to Requirement R1.1 since they are only a component of a communication network. However, NERC defines Cyber Assets as "[p]rogrammable electronic devices and communication networks including hardware, software, and data."[18] NERC's argument rests on the implausible premise that even if a Cyber Asset is subject to the CIP Reliability Standards, the Cyber Asset's components are exempt. We do not agree that the network cabling (i.e., wires) that gives a communication network its networking capability would be exempt from the CIP Reliability Standards. This is especially true in light of NERC's own guidance to industry on the identification of Cyber Assets. Specifically, the NERC *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets* states that "software, data and cabling are considered to exist within the framework of the Cyber Asset and therefore are not separate Cyber Assets themselves."[19] While NERC is correct that wiring is not a stand-alone Cyber Asset, it is clearly a vital component "that exists within the framework of the Cyber Asset" and is subject to the CIP Requirements, where applicable.

16. In addition, as discussed below, the existing interpretation of Requirement R1.1 provides for alternative control measures where strict compliance is not feasible. In light of the existing interpretation, NERC's argument that including the wiring associated with communication networks in the scope of the CIP Reliability Standards would lead to an unintended application of the CIP Reliability Standards and the wasting of limited industry resources is not persuasive.

---

[16] IEEE, *The Authoritative Dictionary of IEEE Standards Terms* (7th ed. 2000).

[17] For example, the International Organization for Standardization (ISO) standards addressing information security management systems require protection of power and communication cabling, i.e., wires. *See* ISO/IEC International Standard 27001, *Information technology – Security techniques – Information security management systems – Requirements*, at 17 (2005).

[18] NERC Glossary, at 4.

[19] NERC, Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets, Version 1.0, at 5 (effective date June 17, 2010), *available at* http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf.

17. An example of the Commission's concern was identified in a recent CIP audit. Specifically, an audit team found cabling between a data center and a control room that was not protected within a six-walled boundary, as required by CIP-006-3d, Requirement R1.1. The cabling was located under unsecured raised floor panels. In this situation, the audit team determined that the two rooms were protected by a single Electronic Security Perimeter due, in part, to the fact that the Registered Entity had not established Electronic Access Points at the border of the two rooms connected by the cabling. Identifying Electronic Access Points is a required step in establishing an Electronic Security Perimeter under CIP-005-3a, Requirement R1.

18. Once a Registered Entity has established a discrete Electronic Security Perimeter by identifying one or more Electronic Access Points, the Registered Entity is required to apply the specific protections outlined in CIP-005-3a. Without those protections in place, the cabling connecting the data center and the control room could be used to access Critical Cyber Assets within either the data center or the control room, unless it is protected by a secure six-walled boundary or alternative physical or logical protections.

19. In this situation, the Registered Entity could have avoided a potential violation by establishing discrete Electronic Security Perimeters around the data center and the control room. At that point, the cabling would be exempt from the CIP Reliability Standards under CIP-002-3b, section 4.2.2. If, for some reason, a Registered Entity could not establish two discrete Electronic Security Perimeters, the existing interpretation of CIP-006-3b, Requirement R1.1, discussed below, provides the flexibility for the adoption of alternative physical and/or logical measures that provide a security equivalent to a six-walled boundary.

20. Accordingly, the Commission finds that NERC's proposed definition of a communication network underlying the instant interpretation is not reasonable in that it is contrary to the general understanding of communication networks and not supported by the Petition.

B. Existing Interpretation of Requirement R1.1

21. In an existing interpretation, NERC addressed a question regarding how Responsible Entities should comply with CIP-006-2, Requirement R1.1 where a completely enclosed border cannot be created around a Cyber Asset. NERC provided the following interpretation:

> *For Electronic Security Perimeter wiring external to a Physical Security Perimeter*, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("six-wall")

> border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.[20]

22. NERC states in the Petition that the existing interpretation did not address whether Requirement R1.1 applies to wires but, rather, the drafting team assumed that the provision applies to wires in the context of explaining the applicability of Requirement R1.1 where a physical border cannot be created around a Cyber Asset. NERC's position, however, is contradicted by both the plain language of the existing interpretation and the petition filed in support of that interpretation.

23. First, by its plain language, the existing interpretation clearly applies to Electronic Security Perimeter *wiring*. Second, NERC states in the petition supporting the existing Commission-approved interpretation that "the interpretation request [in Docket No. RM06-22-000] discusses *connections* between multiple Physical Security Perimeters that reside within a single Electronic Security Perimeter."[21] In addition, NERC states in the prior petition that "several commenters noted disagreement with the standard drafting team's interpretation that wiring is a component of a communication network and needs protection."[22] Notwithstanding such comments, the NERC interpretation explicitly mentions the Requirement's application to wiring external to a Physical Security Perimeter. Thus, the existing interpretation clearly applies to the wiring aspects of communication networks.

24. Therefore, the Commission finds, contrary to NERC's characterization in the instant Petition, that the existing Commission-approved interpretation of Requirement R1.1 of CIP-006-4 specifically addresses the wiring aspects of the communication networks at issue and provides for reasonable alternative compliance measures.

---

[20] Reliability Standard CIP-006-4c (Cyber Security – Physical Security of Critical Cyber Assets), at Appendix 1 (emphasis added).

[21] *North American Electric Reliability Corp.*, Petition, Docket No. RM06-22-000, at 6-7 (filed April 20, 2010) (emphasis added).

[22] *Id.* at 8.

The Commission orders:

NERC's proposed interpretation to Requirement R1.1 of Reliability Standard CIP-006-4 is hereby remanded, as discussed in the body of this order.

By the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.