142 FERC ¶ 61,204
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. RD12-5-000

ORDER ON INTERPRETATION OF RELIABILITY STANDARD

(Issued March 21, 2013)

1. On August 20, 2012, the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), petitioned the Commission to approve an interpretation of Critical Infrastructure Protection (CIP) Reliability Standard CIP-002 (Cyber Security – Critical Cyber Asset Identification). NERC developed the proposed interpretation in response to a request for interpretation of Reliability Standard CIP-002-4 submitted by Duke Energy. For the reasons discussed below, we remand NERC's interpretation.

## I. Background

2. On January 18, 2008, pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Commission issued Order No. 706 approving eight CIP Reliability Standards proposed by NERC, including CIP-002-1.[2] In addition, pursuant to section 215(d)(5) of the FPA,[3] the Commission directed NERC to develop modifications to the CIP Reliability Standards to address certain concerns. Subsequently, the Commission

[1] 16 U.S.C. 824o(d)(2) (2006).

[2] *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).

[3] 16 U.S.C. 824o(d)(5).

approved modifications to the CIP Reliability Standards, including CIP-002-2, CIP-002-3, and CIP-002-4.[4]

3. 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.[5] 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 the team will draft an interpretation of the Reliability Standard, with subsequent balloting.[6] 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

4. In its petition, NERC stated that Duke Energy's interpretation request consisted of the following two questions regarding CIP-002-4, Requirement R3:

> Is the phrase "Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" meant to be prescriptive, i.e., that any and all systems and facilities utilized in monitoring and control, automatic generation control, real-

[4] *North American Electric Reliability Corp*., 128 FERC ¶ 61,291, *order denying reh'g and granting clarification*, 129 FERC ¶ 61,236 (2009) (approving CIP-002-2), *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010) (approving CIP-002-3), *North American Electric Reliability Corp*., 139 FERC ¶ 61,058, *order denying reh'g and clarification*, 140 FERC ¶ 61,109 (2012) (approving CIP-002-4).

[5] NERC Rules of Procedure, Appendix 3A, Reliability Standards Development Procedure, Version 7, at 30 (2010); NERC Rules of Procedure, Appendix 3A, Standard Process Manual, at 27-28 (2010). NERC initially developed the interpretation under Version 7 of the Reliability Standards Development Procedure and later under the Standard Process Manual when it was approved. *See* NERC Petition at 4, n.9.

[6] Under the Reliability Standards Development Procedure, Version 7, the interpretation should be drafted within 45 days, while under the Standard Process Manual a final draft is developed "as soon as practical." Reliability Standards Development Procedure, Version 7, at 30; Standard Process Manual at 27-28.

> time power system modeling, and real-time inter-utility data exchange, must be classified as Critical Cyber Assets, or is this phrase simply meant to provide examples of the types of systems that should be assessed for inclusion in the list of Critical Cyber Assets using an entity's critical cyber asset methodology?
>
> What does the phrase "essential to the operation of the Critical Asset" mean? If an entity has an asset that "may" be used to operate a Critical Asset, but is not "required" for operation of that Critical Asset, is the asset considered "essential to the operation of the Critical Asset"?

5. NERC's proposed interpretation in response to the first question stated that the examples cited in CIP-002 are illustrative and not prescriptive. NERC stated that the interpreted phrase "does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types."[7] NERC responded to the second question as follows:

> The word "essential" is not defined in the Glossary of Terms used in NERC Reliability Standards, but the well-understood meaning and ordinary usage of the word "essential" implies "inherent to" or "necessary." The phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset. A Cyber Asset that "may" be used, but is not "required" (i.e., without which a Critical Asset cannot function as intended), for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3. Similarly, a Cyber Asset that is merely "valuable to" the operation of a Critical Asset, but is not necessary for or inherent to the operation of that Critical Asset, is not "essential to the operation" of the Critical Asset.[8]

6. On August 20, 2012, NERC filed an errata noting that the phrase "[e]xamples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange" was removed from

[7] NERC Petition at 7.

[8] *Id.*

CIP-002-4, and thus the portion of NERC's proposed interpretation in response to the first question only applies to Requirement R3 of CIP-002-1, CIP-002-2, and CIP-002-3. NERC further noted that the phrase "essential to the operation of the Critical Asset" was moved from Requirement R3 in CIP-002-1, CIP-002-2, and CIP-002-3 to Requirement R2 of CIP-002-4.

7. Consistent with NERC's Rules of Procedure, a NERC-assembled ballot body, consisting of industry stakeholders, developed the interpretation initially using the NERC Reliability Standards Development Procedure, Version 7, and subsequently the NERC Standard Process Manual, and the NERC Board of Trustees approved the interpretation.[9] NERC stated that the interpretation does not modify the language contained in the Requirements under review but provides additional clarity with regard to the intent of the Reliability Standard.[10] NERC requested that the Commission approve the interpretation, effective immediately after approval, consistent with the Commission's procedures.

## III. Procedural Matters

8. Notice of NERC's filing was published in the *Federal Register*, 77 Fed. Reg. 47,831 (2012), with interventions and protests due on or before August 22, 2012. Notice of NERC's errata filing was published in the *Federal Register*, 77 Fed. Reg. 54,908 (2012), with interventions and protests due on or before September 4, 2012. Dominion Resources Services, Inc. (Dominion) and Edison Electric Institute filed timely motions to intervene.[11]

## IV. Discussion

### A. Preliminary Matters

9. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.214 (2012), the notices of intervention and timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.

---

[9] *Id.* at 4-5.

[10] *Id.* at 4.

[11] Dominion consists of Virginia Electric and Power Company, Dominion Energy Kewaunee, Inc., Dominion Nuclear Connecticut, Inc., Dominion Energy Brayton Point, LLC, Dominion Energy Manchester Street, Inc., Elwood Energy, LLC, and Kincaid Generation, LLC, and Fairless Energy, LLC.

### B. Commission Determination

10. The Commission remands NERC's proposed interpretation of Reliability Standard CIP-002, for the reasons discussed below. While the Commission agrees with the portion of NERC's interpretation addressing the first question raised by Duke Energy, the Commission does not agree with the portion of NERC's interpretation addressing the second question raised in Duke Energy's interpretation request.[12]

11. The Commission agrees with the part of NERC's interpretation addressing the phrase "[e]xamples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange." That phrase provides a non-exhaustive list of types of systems that should be assessed by registered entities. NERC's interpretation, that the listed items are only illustrative and not prescriptive and that the interpreted phrase "does not imply that the items listed must be classified as Critical Cyber Assets, nor is it intended to be an exhaustive list of Critical Cyber Asset types," is consistent with the use of the term "examples" in CIP-002 and the Commission's understanding.

12. With respect to the second part of NERC's interpretation, the Commission determines that the interpretation misconstrues what is "essential to the operation" of a Critical Asset. This misinterpretation could result in Critical Cyber Assets not being protected by the CIP Reliability Standards, which are currently protected or clearly should be protected under the wording of CIP-002-4, to maintain the operation of associated Critical Assets.[13]

13. In proposing that a cyber asset that "may" be used but is not "required" for the operation of a Critical Asset is not "essential to the operation of the Critical Asset," the proposed interpretation fails to consider that a computer (e.g., a laptop) used by utility

[12] While the Commission agrees with the first part of NERC's interpretation, the two parts of the interpretation were balloted and approved by the NERC Board of Trustees as a single interpretation. *See* NERC Petition at 5. The Commission therefore remands the entire interpretation.

[13] NERC acknowledged this concern in the petition when describing the reasons for negative ballots during the interpretation balloting process. NERC noted that "commenters stated that the interpretation could be construed as restricting the reach of the standard. The interpretation drafting team noted that the interpretation is consistent with the purpose of the standard, but also acknowledged that the proposed interpretation may be construed by the commenters as a restriction on their prior, different understanding of the reach of the standard." NERC Petition at 10.

staff or contractors to control the functions and operations of a Critical Asset is, during such usage, "inherent to or necessary for the operation of a Critical Asset," and thus falls within the scope of CIP-002-4, Requirement R2. Even if the Critical Asset can function at times without human intervention, or such intervention can be done through alternative devices, the device used at any given time to exert such control is "inherent to or necessary for the operation of the Critical Asset."

14. For example, a laptop computer connected to an EMS network through the Internet may be used to supervise, control, optimize, and manage generation and transmission systems, all of which are essential operations.[14] However, the proposed interpretation of "essential" may leave certain cyber assets lacking the required CIP Reliability Standards protection that could, if compromised, affect the operation of associated Critical Assets even though the unprotected cyber assets are using similar access and exerting the same control as cyber assets that are deemed under the proposed interpretation to be "necessary or inherent to the operation of the Critical Asset." The proposed interpretation, in effect, would create a window into the EMS network that could be exploited.

15. The Commission's concerns with remote access are consistent with guidelines developed by NERC in response to Order No. 706.[15] NERC developed two documents: "Security Guideline for the Electric Sector: Identifying Critical Assets" and "Security Guideline for the Electric Sector: Identifying Critical Cyber Assets.[16] The Identifying Critical Cyber Assets document stated that:

> A Cyber Asset could be considered essential to the reliable operation of a Critical Asset, if one or more of the following criteria is met:

---

[14] In one example, a CIP audit found that a registered entity did not identify workstations and laptops as Critical Cyber Assets even though they were being used, via Citrix, to control EMS applications hosted on computers inside the EMS network.

[15] Order No. 706, 122 FERC ¶ 61,040 at P 253.

[16] NERC, Security Guideline for the Electricity Sector: Identifying Critical Assets (2009), *available at* http://www.nerc.com/fileUploads/File/Standards/Reference% 20Documents/Critcal_Asset_Identification_2009Nov19.pdf; NERC, Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets (2010), *available at* http://www.nerc.com/fileUploads/File/ Standards/Critcal%20Cyber%20Asset_approved %20by%20CIPCl%20and%20SC%20for %20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf.

> 1. The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset.
>
> 2. The Cyber Asset displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to the reliable operation of a Critical Asset.
>
> 3. The Cyber Asset fulfills another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the BPS.[17]

16. The Identifying Critical Cyber Assets document also addresses how entities should treat cyber assets that are redundant by stating that:

> Redundancy is not a factor in the determination of the criticality of any Cyber Asset; instead redundancy used to improve reliability and availability may indicate that each redundant Cyber Asset is critical. Because redundancy may increase the opportunities for a successful cyber attack, each Critical Cyber Asset and redundant Critical Cyber Asset should be protected under the Cyber Security Standards as Critical Cyber Assets.[18]

17. In the Commission's view, laptop computers connected to an EMS network through the Internet used to supervise, control, optimize, and manage generation and transmission systems would be "considered essential" under the definition in the Identifying Critical Cyber Assets document.

18. Since the proposed interpretation and petition do not provide adequate justification for leaving unprotected cyber assets (e.g., laptop computers) essential to the operation of associated Critical Assets or explain how this is consistent with Reliability Standard CIP-002-4, Requirement R2, the Commission remands the interpretation.

---

[17] Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets at 7-8.

[18] *Id.* at 8-9.

The Commission orders:

NERC's interpretation of Reliability Standard CIP-002 is hereby remanded, for the reasons discussed in this order.

By the Commission.

( S E A L )

Kimberly D. Bose,
Secretary.