143 FERC ¶ 61,271
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. RD12-5-001

ORDER ON CLARIFICATION

(Issued June 25, 2013)

1. The North American Electric Reliability Corporation (NERC) and Edison Electric Institute (EEI) filed separate requests for clarification of the March 21, 2013 Order on Interpretation of Reliability Standards,[1] in which the Commission remanded NERC's proposed interpretation of Critical Infrastructure Protection (CIP) Reliability Standard CIP-002 (Cyber Security – Critical Cyber Asset Identification).[2] For the reasons discussed in the body of this order, we grant the clarification requests filed by NERC and EEI.

I. Background

2. On August 20, 2012, NERC submitted a proposed interpretation of Reliability Standard CIP-002 for Commission approval (NERC Petition). NERC developed the interpretation in response to a request for interpretation of Reliability Standard CIP-002-4 submitted by Duke Energy. Duke Energy's request for interpretation consisted of the following two questions:

> 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

[1] *North American Electric Reliability Corp.*, 142 FERC ¶ 61,204 (2013) (March 21 Order).

[2] ISO/RTO Council moved to intervene out-of-time and requested clarification or, in the alternative, rehearing of the March 21 Order. As discussed below, we deny the motion to intervene out-of-time and, consequently, ISO/RTO Council's request for clarification or, in the alternative, rehearing.

> 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-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"?

3. In response to the first question, NERC's proposed interpretation 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."[3] In response to the second question, NERC proposed the following interpretation:

> 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.[4]

---

[3] NERC Petition at 7.

[4] *Id.*

4. The March 21 Order agreed with NERC's proposed interpretation in response to the first question 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." The March 21 Order stated that the interpreted phrase provides a non-exhaustive list of types of systems that should be assessed by registered entities. The March 21 Order stated that 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.[5]

5. With respect to the second part of NERC's interpretation, the March 21 Order stated that the proposed interpretation and petition did not provide adequate justification for leaving unprotected cyber assets essential to the operation of associated Critical Assets or explain how doing so would be consistent with Reliability Standard CIP-002-4, Requirement R2. The March 21 Order stated that the interpretation misconstrued what is "essential to the operation" of a Critical Asset and that 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. Specifically, the March 21 Order stated:

> 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 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."
>
> 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

[5] March 21 Order, 142 FERC ¶ 61,204 at P 11.

> systems, all of which are essential operations. 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.[6]

6. The March 21 Order remanded the entire interpretation because the two parts of the interpretation were balloted and approved by the NERC Board of Trustees as a single interpretation.[7]

II. Requests for Clarification or, in the Alternative, Rehearing

7. On April 22, 2013, NERC and EEI each requested clarification of the March 21 Order, while ISO/RTO Council moved to intervene out-of-time and filed a request for clarification or, in the alternative, rehearing of the March 21 Order.

8. NERC seeks clarification of the March 21 Order in two respects. First, NERC requests clarification that "the language in Paragraph 14 of the [March 21 Order] is for illustrative purposes only and is not meant to provide a determination that all laptops must be included in the scope of CIP-002-4, Requirement R2."[8] Second, NERC requests clarification that "references to and discussion of the NERC Guideline Documents in Paragraph 15 of the [March 21 Order] were included for illustrative purposes only rather than forming the basis for the remand, and that the Reliability Standards and requirements determine how a Reliability Standard should be interpreted."[9]

9. EEI seeks clarification that "[NERC-]developed guidelines, such as those cited in the [March 21 Order], are not mandatory and enforceable" and "compliance with CIP-002 will be evaluated on a case-by-case basis, based on the language of the standard and

---

[6] March 21 Order, 142 FERC ¶ 61,204 at PP 13-14 (internal footnotes omitted).

[7] *Id.* P 10 n.12 (citing NERC Petition at 5).

[8] NERC Clarification Request at 2.

[9] *Id.*

the Responsible Entity's individual circumstances, and not on a Responsible Entity's compliance with NERC-developed guidelines."[10] EEI also seeks clarification whether the Commission is "only concerned with laptop computers connected to an EMS network through the Internet used for the functions described in P 17 [i.e., to supervise, control, optimize, and manage generation and transmission systems], or whether it is concerned with the broader description of cyber assets contained in P 14 [i.e., cyber assets that could, if compromised, affect the operation of associated Critical Assets]. If the latter, the Commission should clarify more specifically its intent regarding the description in P 14."[11]

10. ISO/RTO Council seeks clarification of the statement in the March 21 Order that "a computer (e.g., a laptop) used by utility 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."[12] Specifically, ISO/RTO Council seeks clarification or, in the alternative, rehearing that, "contrary to dictating the specific substantive position noted above, the remand order instead intends that NERC is permitted to resubmit an interpretation of CIP-002-4, R2 that does not require all such computers to be identified as [Critical Cyber Assets], as long as that interpretation is sufficiently justified and/or the relationship to the relevant standard/requirement is adequately explained."[13]

III. Discussion

A. Procedural Issues

11. When late intervention is sought after the issuance of a dispositive order, the prejudice to other parties and burden upon the Commission of granting the late intervention may be substantial. Thus, movants bear a higher burden to demonstrate good cause for granting such late intervention. ISO/RTO Council has not met this higher burden of justifying its late intervention. *See, e.g., Midwest Independent Transmission System Operator, Inc.*, 102 FERC ¶ 61,250, at P 7 (2003).

12. In light of our decision to deny ISO/RTO Council's late motion to intervene, we will dismiss ISO/RTO Council's request for clarification or, in the alternative, rehearing.

---

[10] EEI Clarification Request at 1.

[11] *Id.* at 7.

[12] ISO/RTO Council Clarification Request at 6.

[13] *Id.*

Because ISO/RTO Council is not a party to this proceeding, it lacks standing to seek clarification or, in the alternative, rehearing of the March 21 Order under the Federal Power Act and the Commission's regulations. *See* 16 U.S.C. § 825(a) (1994); 18 C.F.R. § 385.713(b) (2012); and *Southern Company Services, Inc.*, 92 FERC ¶ 61,167 (2000).

B. Substantive Issues

13. We grant NERC and EEI's requests for clarification of the March 21 Order.

14. First, we clarify that the March 21 Order did not state that "all laptops must be included in the scope of CIP-002-4, Requirement R2." The March 21 Order stated that "the proposed interpretation fails to consider that a computer (e.g., a laptop) used by utility 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."[14] The March 21 Order further stated that "a laptop computer connected to an EMS network through the Internet *may* be used to supervise, control, optimize, and manage generation and transmission systems" and that "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."[15] As such, the March 21 Order determined that the proposed interpretation and the accompanying petition failed to consider the potential impact of the proposed interpretation on remote access devices that control the functions and operations of Critical Assets or explain how failing to protect such Cyber Assets would be consistent with the language of Reliability Standard CIP-002-4, Requirement R2. We determined only that the proposed interpretation incorrectly excluded cyber assets actually used to control Critical Assets, and this determination was sufficient to warrant a remand. We did not reach the question of whether other cyber assets, such as those capable of controlling Critical Assets, are "essential," and we will reserve judgment on that issue.

15. Second, we clarify that the March 21 Order's reference to the NERC guidelines was intended to illustrate the Commission's concerns with the proposed interpretation. The March 21 Order did not remand the proposed interpretation based on the NERC guidelines nor did the March 21 Order state or imply that the NERC guidelines are mandatory and enforceable. The March 21 Order remanded the proposed interpretation "because the proposed interpretation and petition do not provide adequate justification for leaving unprotected cyber assets essential to the operation of associated Critical Assets or explain how doing so would be consistent with Reliability Standard CIP-002-4,

[14] March 21 Order, 142 FERC ¶ 61,204 at P 13.

[15] *Id.* P 14 (emphases added).

Requirement R2."[16] While the March 21 Order stated that the "Commission's concerns with remote access are *consistent with* guidelines developed by NERC in response to Order No. 706," the March 21 Order did not rely on the NERC guidelines to remand the interpretation.[17]

The Commission orders:

(A) The Commission hereby denies ISO/RTO Council's motion to intervene out-of-time and request for clarification or, in the alternative, rehearing, for the reasons discussed in the body of this order.

(B) The Commission hereby grants NERC and EEI's requests for clarification, for the reasons discussed in the body of this order.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[16] *Id.* P 18.

[17] *Id.* P 15 (emphasis added).