

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Order on Interpretation of Reliability Standard) Docket No. RD12-5-000

**REQUEST FOR CLARIFICATION OF THE
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION**

Pursuant to Rules 212 and 713 of the Federal Energy Regulatory Commission’s (“FERC” or the “Commission”) Rules of Practice and Procedure, 18 C.F.R. § 385.212, 385.713, the North American Electric Reliability Corporation (“NERC”)¹ requests clarification of the Commission’s March 21, 2013 Order on Interpretation of Reliability Standard remanding NERC’s proposed interpretation of CIP-002-4, Requirement R2² (“Remand Order”).³

NERC reiterates the importance of formal interpretations as a tool to help provide clarity about requirements in NERC approved Reliability Standards. Any entity directly and materially affected by Bulk Power System reliability may request an interpretation of a Reliability Standard. In response to such a request, NERC would assemble a team with relevant expertise to address the requested interpretation through the NERC Reliability Standards development process. In the instant case, the interpretation to CIP-002-4, Requirement R2 was developed by a team of foremost experts in the field of Critical Infrastructure Protection to provide clarity on the meaning and intent of CIP-002-4, Requirement R2 based on the language in the Reliability Standard, its requirements, and the CIP-002-4 development record.

¹ The Federal Energy Regulatory Commission certified NERC as the electric reliability organization (“ERO”) in its order issued on July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corporation*, 116 FERC ¶ 61,062 (2006).

² The original interpretation was written for Requirement R3 of CIP-002-3. Due to differences in standard versions, in CIP-002-4, the requirement is R2. For ease of reference, NERC will refer to CIP-002-4, Requirement R2 to identify the interpretation addressed in the Remand Order.

³ *Order on Interpretation of Reliability Standard*, 142 FERC ¶ 61,204 (2013).

I. EXECUTIVE SUMMARY

NERC respectfully requests the following:

- (1) Clarification that the language in Paragraph 14 of the Remand 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.
- (2) Clarification that the Commission's references to and discussion of the NERC Guideline Documents⁴ in Paragraph 15 of the Remand 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.

First, NERC requests the Commission clarify the language in Paragraph 14 of the Remand Order 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, all of which are essential operations" does not mean that *all* laptops are included in the scope of CIP-002-4, Requirement R2.

Second, NERC requests that the Commission clarify that the reference to the Guideline Documents developed by NERC in response to Order No. 706 are merely included in the Remand Order to explain and illustrate the Commission's reasoning and are not meant to form the basis for the Commission's remand of the CIP-002-4, Requirement R2 interpretation.

II. BACKGROUND

On August 1, 2012, NERC submitted a petition for approval of an interpretation of Requirement R3 of Reliability Standard CIP-002-4 (Critical Cyber Asset Identification).⁵ NERC developed the proposed interpretation in response to a request for interpretation submitted by Duke Energy. Duke Energy's request asked two questions: 1) whether certain examples cited in

⁴ *Security Guideline for the Electric Sector: Identifying Critical Assets and Security Guideline for the Electric Sector: Identifying Critical Cyber Assets* ("Guideline Documents")

⁵ *Petition of the North American Electric Reliability Corporation for Approval of an Interpretation to Reliability Standard CIP-002-4 – Critical Cyber Asset Identification*, Docket No. RD12-5-000 (August 1, 2012).

CIP-002 are illustrative and not prescriptive; and 2) for clarification on the meaning of the phrase “essential to the operation of the Critical Asset.” NERC’s interpretation clarified that the examples were illustrative. The interpretation also explained that the phrase “essential to the operation of the Critical Asset” takes on the every-day meaning of “essential” which is “inherent to or necessary” for the operation of the Critical Asset.

FERC remanded the proposed interpretation on March 21, 2013.⁶ In its Remand Order, the Commission agreed with the interpretation response to the first question raised by Duke Energy.⁷ With respect to the second part of the interpretation, the Commission went on to explain that the interpretation misconstrues what is “essential to the operation” of a Critical Asset.⁸ The Commission states 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.⁹ While the Commission did agree with part of the interpretation response, the interpretation was remanded in full.

III. REQUEST FOR CLARIFICATION

A. The Commission Should Clarify that the Language in Paragraph 14 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.

NERC requests the Commission clarify the language in Paragraph 14 of the Remand Order 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, all of which are essential operations” does not mean that *all* laptops are included in the scope of CIP-002-4,

⁶ *North American Electric Reliability Corp.*, 142 FERC ¶ 61,204 (2013).

⁷ Remand Order at P10.

⁸ *Id.* at P12.

⁹ *Id.*

Requirement R2. The Commission’s language in Paragraphs 13 and 14 of the Remand Order are arguably contradictory. In Paragraph 13 of the Remand Order, the Commission states:

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 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.” (*emphasis added*)

That is, Paragraph 13 provides that the laptop must *actually be used* to control the functions and operations of a Critical Asset before it is subject to CIP-002-4, Requirement R2.

In contrast, Paragraph 14 of the Remand Order provides:

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. 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. (*emphasis added*)

The Commission seems to imply in Paragraph 14 that laptops that “*may be used*” to control a Critical Asset should be subject to CIP-002-4, Requirement R2.

The difference in protecting laptops that are *actually used* in ways that are “inherent to or necessary for the operation of a Critical Asset” as compared to laptops that “*may be used* to supervise, control, optimize, and manage generation and transmission systems, all of which are essential operations,” presents a significant difference in compliance and mitigation risk for Responsible Entities. The latter interpretation would essentially require that *all* laptops used in ways that are inherent to or necessary for the operation of a Critical Asset be protected.

FERC seems to recognize this important distinction in Paragraph 17 of the Remand Order, which provides:

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. (*emphasis added*)

NERC assumes that the Commission did not intend that *all* laptops that can be connected in such a way as to supervise, control, optimize, and manage generation and transmission systems be included in the scope of CIP-002-4, Requirement R2. However, in response to certain stakeholder questions, NERC seeks clarification that the language in Paragraph 14 was included for illustrative purposes only.

B. The Commission Should Clarify That the Commission's References to and Discussion of the NERC Guideline Documents in Paragraph 15 were Included for Illustrative Purposes Only and that the Reliability Standards and Requirements Determine how a Reliability Standard Should be Interpreted.

NERC requests the Commission clarify that the reference to the Guideline Documents developed by NERC in response to Order No. 706 are not meant to form the basis for the Commission's remand of the CIP-002-4, Requirement R2 interpretation, but are merely included in the Remand Order as general examples in support of the decision to remand the proposed interpretation, and not as compliance guidance. In addition, in developing interpretations, it is NERC's policy not to modify or expand the requirements outside the scope of the Reliability Standard. In this case, the Commission cited to the Guideline Documents to provide an example of non-standard guidance issued by NERC that is inconsistent with the position espoused in the interpretation. However, these Guideline Documents were developed outside the scope of the Reliability Standard. While the Guideline Documents are important and can provide useful information, the use of guidelines should not take precedent over the language in a Reliability

Standard or its requirements. NERC therefore also seeks clarification that the Commission remand of the proposed interpretation does not signal that the requirements of the standard have been changed.¹⁰

The distinction between the Guideline Documents and CIP-002-4, Requirement R2 is significant because there are subtle, yet important, differences in the language. For example, the Commission cites from the Guideline Documents the following:

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:

- 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. (*emphasis added*)

This language, while important for informational purposes, is broader than the language in the Reliability Standard and requirements. That is, the Guideline Document language that provides that a “Cyber Asset that participates in, *or is capable of*, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset” should not be construed so broadly that *all* laptops that are capable of controlling a Critical Asset are in scope of CIP-002-4, Requirement R2. The language of CIP-002-4, Requirement R2 only provides that Critical Cyber

¹⁰ In developing the proposed interpretation, the Interpretation Drafting Team did not use the Guideline Documents to form the basis of its proposed interpretation. In fact, NERC’s petition did not reference the Guideline Documents. They were only limitedly referenced in the Standards Development History in response to comments that addressed one of the Guideline Documents. The summary of comments provides:

One commenter believed that the clarification provided for essential is much narrower than the guidance provided in the Security Guideline for the Electricity Sector: *Identifying Critical Cyber Assets*, and that the interpretation does not provide additional clarity than what is provided in the existing guideline. The IDT understands that many entities already understood or interpreted this requirement similarly to the interpretation’s response, and to those entities, this interpretation may at first seem unnecessary. However, the interpretation provides necessary clarity for all entities.

Assets that *are essential* to the operation of the Critical Asset, not those that *could be essential*, be included in the list of Critical Assets:

R2. Critical Cyber Asset Identification— Using the list of Critical Assets developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. The Responsible Entity shall update this list as necessary, and review it at least annually.

For this reason, NERC requests that the Commission provide clarification that its references to and discussion of the NERC Guideline Documents in Paragraph 15 of the Remand 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.

IV. CONCLUSION

For the reasons set forth herein, NERC requests that the Commission clarify its language in Paragraphs 14 and 15 of the Remand Order.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability
Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595– facsimile

/s/ Holly A. Hawkins

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Assistant General Counsel
Stacey Tyrewala
Senior Counsel
North American Electric Reliability
Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099– facsimile
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
stacey.tyrewala@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

Dated: April 22, 2013

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 22nd day of April, 2013.

/s/ Holly A. Hawkins

Holly A. Hawkins

Assistant General Counsel for North

American Electric Reliability Corporation