ONTARIO ENERGY BOARD
OF THE PROVINCE OF ONTARIO

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF AN INTERPRETATION TO RELIABILITY STANDARD CIP-002-3—CRITICAL CYBER ASSET IDENTIFICATION AND CIP-002-4 – CRITICAL CYBER ASSET IDENTIFICATION

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

August 27, 2012

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC") hereby requests approval of an interpretation of Reliability Standard CIP-002-3 – Critical Cyber Asset Identification, Requirement R3 and CIP-002-4 — Critical Cyber Asset Identification, Requirement R2, to become effective concurrent with the date of approval of this petition.[1] The proposed interpretation is set forth in **Exhibit A** to this petition. Upon approval of the interpretation, the standard will be referred to as CIP-002-3a – Critical Cyber Asset Identification and CIP-002-4a — Critical Cyber Asset Identification.

On January 31, 2010, Duke Energy requested a formal interpretation of CIP-002-1 Cyber Security – Critical Cyber Asset Identification, Requirement R3.[2] The NERC-assembled interpretation drafting team prepared the proposed response to the request for interpretation, which has been approved by the NERC Board of Trustees. No modification to the language contained in this specific Reliability Standard requirement is being proposed through the interpretation.

---

[1] As further explained below, Duke Energy's proposed interpretation makes reference to 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," which is included in Requirement R3 of CIP-002-1, CIP-002-2, and CIP-002-3. However, this phrase was modified in CIP-002-4, and the requirement no longer includes examples. Therefore, with respect to the above phrase, the interpretation of CIP-002 applies only to CIP-002-1, CIP-002-2, and CIP-002-3, and does not apply to CIP-002-4. In addition, due to the renumbering of requirements in CIP-002-4, the word "essential" referenced in the proposed interpretation now appears in Requirement R2 of CIP-002-4. However, in CIP-002-1, CIP-002-2, and CIP-002-3, the word "essential" is found in Requirement R3.

[2] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was in effect. The request for the interpretation for Requirement R3 of CIP-002-1 sought clarity on what types of systems must be classified as Critical Cyber Assets and to provide clarity on the phrase "essential to the operation of the Critical Asset." The request was therefore processed referencing CIP-002. Subsequently, Versions 2, 3 and 4 of the CIP standards were submitted. Except as explained in footnote 1, above, the changes in Versions 2, 3, and 4, relative to Version 1 of CIP-002, are not material to the substance of the interpretation request. Given that Version 3 is currently-effective, and Version 4 will become effective on April 1, 2014, NERC will append the requested interpretation to Version 3 or Version 4 of the CIP-002 standard, whichever is in effect at the time of approval of this interpretation, in lieu of Version 1.

Exhibit A to this petition sets forth the interpretation of Requirement R3 to CIP-002-3 and Requirement R2 to CIP-002-4. **Exhibit B** contains proposed Reliability Standard CIP-002-3a and CIP-002-4a — Critical Cyber Asset Identification, which includes the appended interpretation of Requirement R3 and Requirement R2, respectively. **Exhibit C** to this petition contains the drafting team's consideration of industry comments for the interpretation. **Exhibit D** contains the complete development history of the Interpretation. **Exhibit E** to this petition contains the roster of the interpretation drafting team that drafted the interpretation.

NERC filed this interpretation with the Federal Energy Regulatory Commission ("FERC"), and is also filing this interpretation with the other applicable governmental authorities in Canada.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

III. BACKGROUND

a. Basis for Approval of Proposed Reliability Standard Interpretation

The proposed interpretation is of a requirement contained within a Reliability Standard, but does not represent a new or modified Reliability Standard. However, the proposed Reliability Standard interpretation provides additional clarity with regard to the intent of the Reliability Standard. Therefore, NERC requests approval of the proposed interpretation.

b. Reliability Standards Development Procedure and Interpretation

All persons who are directly or materially affected by the reliability of the North American bulk power system are permitted to request an interpretation of a Reliability Standard, as discussed in NERC's *Standard Processes Manual,* which is incorporated into the NERC Rules of Procedure as Appendix 3A.

A valid interpretation request is one that requests additional clarity about one or more requirements in a Reliability Standard and does not request verification as to whether or not a specific approach will be judged as complying with one or more requirements in a Reliability Standard. A valid interpretation in response to a request for interpretation provides additional clarity about one or more requirements within a Reliability Standard, but does not expand or limit the Reliability Standard or any of its requirements beyond the language contained in the standard.

The process for responding to a valid request for interpretation requires NERC to assemble a team with the relevant expertise to address the interpretation request. The interpretation drafting team is then required to draft a response to the request for interpretation and then present that response for industry ballot. If approved by the ballot pool and the NERC Board of Trustees, the interpretation is appended to the Reliability Standard and filed for approval by FERC and applicable governmental authorities in Canada. Then, when the affected Reliability Standard undergoes its next substantive revision, the interpretation will be incorporated into the Reliability Standard, as appropriate.

The proposed interpretation, as set out in **Exhibit A**, was approved by a ballot pool on April 30, 2012, with a weighted segment approval of 94.71 percent.[3] The proposed interpretation was approved by the NERC Board of Trustees on May 9, 2012.

[3] The interpretation drafting team's considerations of comments for the interpretation is contained in **Exhibit C**. The complete development record for the interpretation, including the ballot pool, the final ballot results by registered ballot body members, stakeholder comments received during the balloting, and an explanation of how those comments were considered are set forth in **Exhibit D**.

IV. Proposed CIP-002-3a – Critical Cyber Asset Identification Interpretation and CIP-002-4a—Critical Cyber Asset Identification Interpretation

In Section IV(a), below, NERC summarizes the justification for the proposed interpretation of Requirement R3 of CIP-002-3 and Requirement R2 of CIP-002-4, and explains the development of the interpretation. Section IV(b) summarizes the development proceedings for this interpretation and explains how stakeholder comments were addressed by the interpretation drafting team.

a. Justification for Approval of Interpretation

The stated purpose of CIP-002 is the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. Requirement R3 of CIP-002-1 provided[4]:

> **R3.** Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. 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. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> **R3.1**. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> **R3.2** The Cyber Asset uses a routable protocol within a control center; or,

[4] As explained, above, 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," is included in Requirement R3 of CIP-002-1, CIP-002-2, and CIP-002-3. However, this phrase was modified in CIP-002-4, and the requirement no longer includes examples. In addition, due to the renumbering of requirements in CIP-002-4, the word "essential" referenced in the proposed interpretation now appears in Requirement R2 of CIP-002-4. However, in CIP-002-1, CIP-002-2, and CIP-002-3, the word "essential" is found in Requirement R3.

R3.3 The Cyber Asset is dial-up accessible.

In its interpretation request, Duke Energy sought clarification with respect to specific language in CIP-002-1, Requirement 3:

1. 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-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?

2. 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"?

In response to the Duke Energy request, the interpretation drafting team developed, and the industry stakeholders approved, the following interpretation:[5]

> 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" is illustrative, not prescriptive. It simply provides examples of the types of Cyber Assets that should be considered. It 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.
>
> 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

[5] The interpretation drafting team was provided the guidelines for drafting interpretations in force at the time the interpretation was developed.

> 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.

As discussed below, the proposed interpretation of Requirement R3 of CIP-002-3 and of Requirement R2 of CIP-002-4 are consistent with the stated purpose of the Reliability Standard, which is to support the reliable operation of the Bulk Electric System by identifying and documenting Critical Cyber Assets associated with Critical Assets, because it ensures that assets that are essential to the operation of Critical Assets are subject to compliance with the standard.

The first paragraph of the interpretation addresses the examples of Critical Cyber Assets that a Responsible Entity should consider during the identification and documentation process. The interpretation clarifies that the list of examples provided in Requirement R3 of CIP-002-3 are illustrative of the types of Cyber Assets that may be Critical Cyber Assets, and that the examples do not represent an exhaustive list of Critical Cyber Asset types.

Indeed, there are Critical Assets that are not included in the list of examples that could be identified by a Responsible Entity as Critical Cyber Assets, and there are Critical Assets that are included in the list of examples that may not otherwise meet the criteria for identification as Critical Cyber Assets. Therefore, the interpretation clarifies that the examples listed in Requirement R3 of CIP-002-3 are not prescriptive.

In the second paragraph, the proposed interpretation clarifies the meaning of the language "essential to the operation of the Critical Asset" in Requirement R3 of CIP-002-3 and Requirement R2 of CIP-002-4. Applying the common meaning of the word

essential, the interpretation drafting team determined that the phrase "essential to the operation of the Critical Asset" means inherent to or necessary for the operation of the Critical Asset.[6] Applying the standard to these essential assets will ensure that Critical Cyber Assets associated with Critical Assets are properly identified and addressed by the standard.

Consistent with the purpose of Requirement R3 of CIP-002-3 and Requirement R2 of CIP-002-4, a Cyber Asset that "may" be used, but is not "required" for the operation of a Critical Asset, is clearly not "essential" to the operation of the Critical Asset. As such, Requirement R3 of CIP-002-3 and Requirement R2 of CIP-002-4 are intended to identify and document those Cyber Assets that are necessary for or inherent to the operation of the Critical Asset.

b. Summary of the Reliability Standard Development Proceedings

NERC presented the proposed interpretation for a first initial ballot from March 14, 2012, through March 23, 2012, and it achieved a quorum of 89.63 percent, with a weighted affirmative approval of 94.71 percent. There were seven negative ballots submitted in the initial ballot, and three of those included a comment, which initiated the need for a recirculation ballot.

A second draft interpretation was developed and posted for recirculation ballot from April 20, 2012, to April 30, 2012. Stakeholders supported the draft interpretation, which achieved a quorum of 92.68 percent with a weighted affirmative approval of 94.61

[6] *See* Merriam-Webster's Dictionary (2012) (defining essential as: "1: of, relating to, or constituting essence: inherent.") available at: http://www.merriam-webster.com/dictionary/essential.

percent. There were 8 negative ballots submitted in the second initial ballot, and four of those ballots included a comment.

As demonstrated in the summary of comments presented below, a minority of commenters noted disagreement with certain aspects of the proposed interpretation, and some balloters commented on more than one issue. Specifically, reasons cited for negative ballots included the following:

- With respect to the response to Question 1, commenters disagreed that the types of Cyber Assets provided in the example "should be considered" and noted that the language "should be considered" is not found in CIP-002-3, Requirement R3, and should not be inferred. The interpretation drafting team explained, and a majority of commenters agree, however, that the examples do not imply that the items listed as examples in the requirement must be classified as Critical Cyber Assets, which requires some "consideration" within the context of the requirement.
- With respect to the response to Question 2, 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.
- With respect to the response to Question 2, commenters stated that the interpretation is unnecessary because "essential" is defined in collegiate dictionaries and there is no technical basis for adding clarity to or better

defining this term, either in an interpretation or in the *NERC Glossary of Terms*. The interpretation drafting team disagreed because the proposed interpretation clarifies the meaning of "essential" as it applies to the purpose of this standard.

c. Future Action

The currently effective CIP-002-3 Reliability Standard was submitted on January 21, 2010. Reliability Standard CIP-002-4 was submitted on June 8, 2011, and will become effective on April 1, 2014. Upon approval of the requested interpretation, the interpretation shall remain in effect until such time as the interpretation can be incorporated into a future revision of the standard.

V. Conclusion

NERC respectfully requests approval of the interpretation to Reliability Standard CIP-002-3—Critical Cyber Asset Identification, Requirement R3 and CIP-002-4 Cyber Security – Critical Cyber Asset Identification, Requirement R4, as set out in **Exhibit A**. NERC requests that this interpretation be made effective immediately upon approval.

Respectfully submitted,

/s/ Willie L. Phillips
Willie L. Phillips

Gerald W. Cauley
President and Chief Executive Officer
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
charlie.berardesco@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection
North American Electric Reliability Corporation

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

EXHIBITS A -E

(Available on the NERC Website at
http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP-002_Interp_Filing)