BEFORE THE
BRITISH COLUMBIA UTILITIES COMMISSION
OF THE PROVINCE OF BRITISH COLUMBIA

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

NOTICE OF FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION OF AN INTERPRETATION TO RELIABILITY STANDARD CIP-004-4 – PERSONNEL AND TRAINING

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 provides notice of an interpretation of Reliability Standard CIP-004-4a[1] — Personnel and Training, Requirements R2, R3, and R4, to become effective as set forth in **Exhibit A**. The standard will be referred to as CIP-004-4a — Personnel and Training.

On October 15, 2009, the Western Electricity Coordinating Council ("WECC") requested a formal interpretation of CIP-004-1, Requirements R2, R3, and R4.[2] The NERC-assembled interpretation drafting team developed the proposed response to the WECC request for interpretation of Requirements R2, R3, and R4 of CIP-004-4, which has been approved by the NERC Board of Trustees. No modification to the language contained in the specific Reliability Standard requirements is being proposed through the interpretation.

Exhibit A to this notice sets forth the proposed interpretation of Requirements R2, R3, and R4 to CIP-004-4. **Exhibit B** to this notice contains Reliability Standard CIP-004-4a — Personnel and Training, which includes the appended interpretation of Requirements R2, R3, and R4. **Exhibit C** to this notice contains the drafting team's consideration of industry comments for the interpretation. **Exhibit D** contains the complete development history of the interpretation. **Exhibit E** contains the roster of the interpretation drafting team.

---

[1] The proposed interpretation applies to versions 1, 2, 3, and 4 of the standard. For purposes of this filing, the standard will be referred to as CIP-004-4.

[2] At the time this request for interpretation was submitted to NERC, Version 1 of the CIP standards was in effect. The request was therefore processed referencing CIP-004-1. Subsequently, Versions 2, 3 and 4 of the CIP standards were submitted. However, the changes in Versions 2, 3, and 4, relative to Version 1 of CIP-004, 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-004 standard, whichever is in effect.

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

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

III. BACKGROUND

a. Basis of Proposed Reliability Standard Interpretation

The proposed interpretation is of requirements 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.

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.

The proposed interpretation to CIP-004-4, Requirements R2, R3, and R4, as set out in **Exhibit A**, was approved by a ballot pool on April 30, 2012, with a weighted

segment approval of 80.08 percent.[3] The proposed interpretation was approved by the NERC Board of Trustees on May 9, 2012.

IV. Proposed CIP-004-4a—Personnel and Training Interpretation

In Section IV(a), below, NERC summarizes the justification for the proposed interpretation of Requirements R2, R3, and R4 of CIP-004-4, 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 of Interpretation

The stated purpose of CIP-004-4 calls for personnel that have authorized cyber or authorized unescorted physical access to Critical Cyber Assets to have an appropriate level of personnel risk assessment, training, and security awareness. Requirements R2, R3, andR4 of CIP-004-4 state:

> **R2.** Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
>
> **R2.1.** This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.
>
> **R2.2.** Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

[3] The interpretation drafting team's considerations of comments for the interpretation of Requirements R2 through R4 is contained in **Exhibit** C. The complete development record for the interpretation, including the requests for the interpretation, the responses to the requests for the interpretation, the ballot pool, and 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**.

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

> **R4.2.** The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

In its interpretation request, WECC sought clarification on the definition of "authorized access" as applied to temporary support from vendors. In response to the WECC request, the interpretation drafting team developed, and the industry stakeholders approved, the following interpretation:[4]

> The drafting team interprets that a vendor may be granted escorted physical access to Critical Cyber Assets; however, for a vendor to be granted authorized cyber access, the vendor must complete the risk assessment and training as required by CIP-004-1 Requirement R2. CIP-003-1 Requirement R3 permits exceptions to an entity's cyber security policy, such as for an event requiring emergency access. It is recognized that the cited question and answer from the Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training document states that "…some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training." However, this particular guidance should be revisited. For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. It is further noted that an FAQ is not a standard, and cannot create or dilute the language of the standard itself.

The above interpretation addresses whether training, risk assessment, and access requirements specified in CIP-004-4, Requirements R2, R3, and R4, are applicable to supervised personnel. The interpretation clarifies that an individual can be granted supervised *physical* access to Critical Cyber Assets, and, under those circumstances, Requirements R2 R3, and R4 would not apply. However, CIP-004-4 does not distinguish between "supervised" and "unescorted" *cyber* access. Therefore, the interpretation

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

clarifies that all cyber access must be authorized. And all authorized cyber access requires compliance with Requirements R2, R3, and R4 of CIP-004-4. To put it another way, any cyber access, whether "supervised" or not, must be authorized pursuant to CIP-004-4 requirements.

If supervised cyber access were allowed without meeting the authorization requirements, it could potentially expose Critical Cyber Assets to harm by individuals who have not received the proper personnel risk assessment, training, and security awareness. Thus, the proposed interpretation of Requirements R2, R3, and R4 of CIP-004-4 is consistent with the stated purpose of the Reliability Standard.

b. Summary of Interpretation Development Proceedings

NERC presented the proposed interpretation for a first initial ballot from December 7, 2009, through January 6, 2010, and achieved a quorum of 84.21 percent with a weighted affirmative approval of 42.24 percent. There were 106 negative ballots submitted in the initial ballot, and 85 of those ballots included a comment, which initiated the need for another initial ballot.

A second draft interpretation was developed and posted for initial ballot from February 27, 2012, to March 23, 2012. Stakeholders supported the draft interpretation, which achieved a quorum of 88.55 percent, with a weighted affirmative approval of 79.61 percent. There were 65 negative ballots submitted in the second initial ballot, and 41 of those ballots included a comment; however, work on the interpretation was delayed based on reprioritization of the total standards workload in accordance with guidance from NERC Board of Trustees issued November 2009.

In April 2011, the Standards Committee approved and issued the *NERC Guidelines for Interpretation Drafting Teams*, and the Standards Committee directed that work resume on the interpretation. A project team assembled from members of the standing CIP interpretation drafting team reviewed and responded to the comments received during the last successive ballot and made revisions to the interpretation.

A recirculation ballot was held from April 20, 2012, to April 30, 2012, and the interpretation was approved by stakeholders, achieving 80.08 percent approval with a quorum of 90.96 percent.

As demonstrated in the summary of comments presented below, some commenters noted disagreement with the determination that all electronic or cyber access must be authorized pursuant to CIP-004-4 requirements, and some balloters commented on more than one issue. The reasons cited for negative ballots include the following:

- Commenters disagreed with how the interpretation addresses supervised cyber and physical access separately for vendors. The interpretation drafting team and majority of balloters agree, however, that the standard language treats electronic and physical access separately by including the word "unescorted" only in reference to physical access. The standard does not use "unescorted" in reference to electronic or cyber access.
- Commenters stated that typing on a keyboard is physical access, and that physical access loses any meaning and would no longer be necessary if escorted physical access did not allow physical interaction with the device. In response, however, the interpretation drafting team stated, and balloters agree, that it does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access, which requires authorization.
- Commenters stated that the absence of language in the standard regarding supervision of electronic access does not absolutely prohibit the concept. While Requirement R2 does not explicitly exclude the concept of "escorting" individuals with electronic access, it does not include a provision for "escorted" electronic access either. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to CIP-004-4 requirements.
- Commenters stated that the interpretation does not allow for emergency access when needed. The interpretation drafting team notes, however, that Versions 2, 3, and 4 of CIP-004 allows an exception to the training and personnel assessment authorization requirements, under certain circumstances, including emergency situations.

- Commenters stated that the interpretation may increase the risk to the Bulk Electric System. However, considering the provisions for emergency and planned access, this interpretation does not increase the risk level to the Bulk Electric System.

c. Future Action

The currently effective CIP-004-3 Reliability Standard was submitted on January 21, 2010. Reliability Standard CIP-004-4 was submitted on June 8, 2011, and will become effective on April 1, 2014. The requested interpretation shall remain in effect until such time as the interpretation can be incorporated into a future revision of the standard.

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

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

EXHIBITS A – E

(Available on the NERC Website at
http://www.nerc.com/fileUploads/File/Filings/Attachments_CIP-004_Interp_Filing)