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

| | | |
|---|---|---|
| **NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION** | **)** **)** | **Docket No. RD12-__-000** |

# PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL 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 1, 2012

## TABLE OF CONTENTS

## I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby requests the Federal Energy Regulatory Commission ("FERC" or "Commission") approve, in accordance with Section 215(d)(1) of the Federal Power Act ("FPA")[2] and Section 39.5 of FERC's Regulations,[3] an interpretation of Reliability Standard CIP-004-4a[4] — Personnel and Training, Requirements R2, R3, and R4, to become effective concurrent with the date of a FERC Order approving this petition, as set forth in **Exhibit A**. Upon Commission approval of the interpretation, 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.[5] 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

[1] NERC was certified by FERC as the electric reliability organization ("ERO") authorized by Section 215 of the Federal Power Act. FERC certified NERC as the ERO in its order issued July 20, 2006 in Docket No. RR06-1-000 *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing,* 116 FERC ¶ 61,062 (2006) ("ERO Certification Order").

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

[3] 18 C.F.R. § 39.5 (2011).

[4] 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.

[5] 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 approved by FERC. 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 at the time of FERC approval of this interpretation, in lieu of Version 1. *See Order Approving Revised Reliability Standards for Critical Infrastructure Protection and Requiring Compliance Filing,* 128 FERC ¶ 61,291 (September 30, 2009); *Order on Compliance,* 130 FERC ¶ 61,271 (2010) (March 31, 2010); *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 139 FERC ¶ 61,058 (April 19, 2012).

contained in the specific Reliability Standard requirements is being proposed through the interpretation.

**Exhibit A** to this petition sets forth the proposed interpretation of Requirements R2, R3, and R4 to CIP-004-4. **Exhibit B** to this petition contains Reliability Standard CIP-004-4a — Personnel and Training, which includes the appended interpretation of Requirements R2, R3, and R4. **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** contains the roster of the interpretation drafting team.

NERC is also filing this interpretation with applicable governmental authorities in Canada.

## II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[6]


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. Regulatory Framework

By enacting the Energy Policy Act of 2005,[7] Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system, and with the duties of certifying an electric reliability organization ("ERO") that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. Section 215 states that all users, owners and operators of the bulk power system in the United States will be subject to FERC-approved Reliability Standards.

[6] Persons to be included on FERC's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[7] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005) (codified at 16 U.S.C. § 824o).

### b. Basis for Approval of Proposed Reliability Standard Interpretation

The proposed interpretation is of requirements contained within a Commission-approved 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 that the Commission approve the proposed interpretation.

### c. 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*,[8] 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 regulatory-approved 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 regulatory-approved 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

[8] Note that FERC approved the new *Standard Processes Manual* in the Commission's *Order Approving Petition and Directing Compliance Filing*, 132 FERC ¶ 61,200 (2010), which replaced the NERC's *Reliability Standards Development Procedure Version 7* in its entirety. NERC developed these interpretations in accordance with the *Reliability Standards Development Procedure Version 7* until the *Standard Processes Manual* was approved on September 3, 2010. NERC's *Reliability Standards Development Procedure* is available on NERC's website at: http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf. The Standard Processes Manual is available at: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf.

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.[9] 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.

[9] 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**.

**a. Justification for Approval 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:
>
> **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:[10]

> 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

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

> 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 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 approved by the Commission on March 31, 2010.[11] Reliability Standard CIP-004-4 was approved by the Commission on April 19, 2012, and will become effective on April 1, 2014.[12] Upon Commission 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.

[11] *North American Electric Reliability Corp.*, 130 FERC ¶ 61,271 (2010).
[12] *Version 4 Critical Infrastructure Protection Reliability Standards*, 139 FERC ¶ 61,058 (2012).

## V. Conclusion

NERC respectfully requests that FERC approve the interpretation to FERC-approved Reliability Standard CIP-004-4 — Personnel and Training, Personnel and Training, Requirements R2, R3, and R4, as set out in **Exhibit A**, in accordance with Section 215(d)(1) of the FPA and Part 39.5 of FERC's regulations. NERC requests that this interpretation be made effective immediately upon issuance of FERC's order in this proceeding.

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

## 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 1st day of August, 2012.

*/s/ Willie L. Phillips*
Willie L. Phillips
*Attorney for North American Electric Reliability Corporation*

## Exhibit A

Interpretation of Requirements R2, R3, and R4 of CIP-004-4 — Personnel and Training.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Note: an Interpretation cannot be used to change a standard.**

| Request for an Interpretation of a Reliability Standard |
|---|
| Date submitted: 10/15/09 |
| Date accepted: 10/23/09 |
| **Contact information for person requesting the interpretation:** |
| Name: John Van Boxtel |
| Organization: Western Electricity Coordinating Council |
| Telephone: 360-713-9090 |
| E-mail: jvanboxtel@wecc.biz |
| **Identify the standard that needs clarification:** |
| Standard Number: CIP-004-1 |
| Standard Title: Cyber Security – Personnel and Training |
| **Identify specifically what requirement needs clarification:** |

**Requirement Number and Text of Requirement:** R2, R3, and R4

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

**Clarification needed (emphasis added):**

Specifically, the WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would

temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

**Background**

Through previously published documents, both NERC and FERC have indicated that the intent of the CIP-004 Standard was to document training, risk assessment, and access to Critical Cyber Assets in situations where personnel have direct and unmonitored access to critical cyber assets, as opposed to and distinguishable from **supervised access.**

The question asked in Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training is: "*What is meant by 'authorized cyber access?'" The answer provided is:*

> *The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.* (emphasis added)

This answer is also consistent with a similar description of escorted access provided in FERC Order 706, page 116, paragraph 432, in which the Commission stated:

> *Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power system. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.* (emphasis added)

**Identify the material impact associated with this interpretation:**

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

**Material Impact**

If "Authorized Access" includes temporary support access provided in a supervised manner, then there is a potential for many Registered Entities to either be noncompliant while seeking support, or excessively burdened by limiting access to timely support. This situation is particularly likely from large non-utility vendors (such as Cisco Systems) that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard.

Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations:

- Training covering the specific policies, access controls, and procedures as developed by each individual Registered Entity.
- A personnel risk assessment for all support personnel provided by each individual vendor, based on the cyber security training program developed by each individual Registered Entity.
- Timely updates to each Registered Entity's access list of all support personnel provided by each individual vendor, including changes in personnel at the vendor within the timeframes prescribed by the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

## Project 2009-26: Response to Request for an Interpretation of NERC Standard CIP-004-1 for the Western Electricity Coordinating Council

The following interpretation of NERC Standard CIP-004-1 Cyber Security — Personnel & Training, Requirements R2, R3, and R4, was developed by the Cyber Security Order 706 SAR drafting team.

### Requirement Number and Text of Requirement

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

### Question

The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

### Response

WECC asks three questions, which are listed below. The answer to each question follows the question.

1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

   Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.

2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?

**Exhibit B**

Proposed Reliability Standards CIP-004-3a and CIP-004-4a — Personnel and Training, that includes the appended interpretation of Requirements R2, R3, and R4, submitted for approval.

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

## A. Introduction

**1. Title:** Cyber Security — Personnel & Training

**2. Number:** CIP-004-3a

**3. Purpose:** Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

**4. Applicability:**

**4.1.** Within the text of Standard CIP-004-3, "Responsible Entity" shall mean:

**4.1.1** Reliability Coordinator.

**4.1.2** Balancing Authority.

**4.1.3** Interchange Authority.

**4.1.4** Transmission Service Provider.

**4.1.5** Transmission Owner.

**4.1.6** Transmission Operator.

**4.1.7** Generator Owner.

**4.1.8** Generator Operator.

**4.1.9** Load Serving Entity.

**4.1.10** NERC.

**4.1.11** Regional Entity.

**4.2.** The following are exempt from Standard CIP-004-3:

**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.3** Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

**5. Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

**R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

**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:

**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.

## C. Measures

**M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

**M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

**M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

**M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

**1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

**1.1.2** ERO for Regional Entity.

**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### 1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

**1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information**

**2. Violation Severity Levels (To be developed later.)**

## E. Regional Variances

None identified.

## Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 01/16/06 | D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…" | 03/24/06 |
| 1 | 06/01/06 | D.2.1.4 — Change "access control rights" to "access rights." | 06/05/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Reference to emergency situations.<br>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.<br>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.<br>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".<br>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Update version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by NERC Board of Trustees | Update |
| 3a | 5/24/12 | Interpretation of R2, R3, and R4 adopted by NERC | |

| | | | |
|---|---|---|---|
| | | Board of Trustees | |

**Appendix 1**

| **Requirement Number and Text of Requirement** |
|---|
| R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.<br><br>R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.<br><br>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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:<br><br>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. |
| **Question 1** |
| The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? |
| **Response to Question 1** |
| WECC asks three questions, which are listed below. The answer to each question follows the question.<br><br>1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.<br><br>2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? |

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

## A. Introduction

**1. Title:** Cyber Security — Personnel & Training

**2. Number:** CIP-004-33a

**3. Purpose:** Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

**4. Applicability:**

**4.1.** Within the text of Standard CIP-004-3, "Responsible Entity" shall mean:

**4.1.1** Reliability Coordinator.

**4.1.2** Balancing Authority.

**4.1.3** Interchange Authority.

**4.1.4** Transmission Service Provider.

**4.1.5** Transmission Owner.

**4.1.6** Transmission Operator.

**4.1.7** Generator Owner.

**4.1.8** Generator Operator.

**4.1.9** Load Serving Entity.

**4.1.10** NERC.

**4.1.11** Regional Entity.

**4.2.** The following are exempt from Standard CIP-004-3:

**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.3** Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

**5. Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

**R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);

- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

**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:

**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.

## C. Measures

**M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

**M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

**M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

**M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

**1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

**1.1.2** ERO for Regional Entity.

**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### 1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

**1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

**1.5. Additional Compliance Information**

**2. Violation Severity Levels (To be developed later.)**

## E. Regional Variances

None identified.

## Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 01/16/06 | D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…" | 03/24/06 |
| 1 | 06/01/06 | D.2.1.4 — Change "access control rights" to "access rights." | 06/05/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Reference to emergency situations.<br>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.<br>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.<br>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".<br>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Update version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by NERC Board of Trustees | Update |
| 3a | 5/24/12 | Interpretation of R2, R3, and R4 adopted by NERC | |

| | | | |
|---|---|---|---|
| | | Board of Trustees | |

## Appendix 1

| Requirement Number and Text of Requirement |
|---|
| R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.<br><br>R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.<br><br>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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:<br><br>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. |
| **Question 1** |
| The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? |
| **Response to Question 1** |
| WECC asks three questions, which are listed below. The answer to each question follows the question.<br><br>1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.<br><br>2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? |

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

## A. Introduction

**1. Title:** Cyber Security — Personnel & Training

**2. Number:** CIP-004-4a

**3. Purpose:** Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

**4. Applicability:**

**4.1.** Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

**4.1.1** Reliability Coordinator.

**4.1.2** Balancing Authority.

**4.1.3** Interchange Authority.

**4.1.4** Transmission Service Provider.

**4.1.5** Transmission Owner.

**4.1.6** Transmission Operator.

**4.1.7** Generator Owner.

**4.1.8** Generator Operator.

**4.1.9** Load Serving Entity.

**4.1.10** NERC.

**4.1.11** Regional Entity.

**4.2.** The following are exempt from Standard CIP-004-4:

**4.2.1** Facilities regulated by the Canadian Nuclear Safety Commission.

**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.3** In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

**4.2.4** Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

**5. Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

**R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound

security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

**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-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

**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-004-4.

**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.

## C. Measures

**M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

**M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

**M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

**M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

#### 1.2. The RE shall serve as the CEA with the following exceptions:

**1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

**1.2.2** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

**1.2.3** For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

**1.2.4** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

**1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.5. Additional Compliance Information

### 2. Violation Severity Levels

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|---|---|---|---|---|---|
| R1. | LOWER | The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices. | The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis. | The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. | The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. |
| R2. | LOWER | The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. | The Responsibility Entity did not review the training program on an annual basis. | The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. | The Responsible Entity did not establish, document, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. |
| R2.1. | MEDIUM | At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. | At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. | At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. | 15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. |

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|---|---|---|---|---|---|
| R2.2. | MEDIUM | N/A | The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4. | The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4. | The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4. |
| R2.2.1. | LOWER | N/A | N/A | N/A | N/A |
| R2.2.2. | LOWER | N/A | N/A | N/A | N/A |
| R2.2.3. | LOWER | N/A | N/A | N/A | N/A |
| R2.2.4. | LOWER | N/A | N/A | N/A | N/A |
| R2.3. | LOWER | N/A | N/A | The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records. | The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records. |
| R3. | MEDIUM | N/A | The Responsible Entity has a 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, but the program is not documented. | The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency. | The Responsible Entity does not 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.<br><br>OR<br><br>The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency. |
| R3.1. | LOWER | N/A | N/A | The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check. | The Responsible Entity did not 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. |

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|---|---|---|---|---|---|
| R3.2. | LOWER | N/A | The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable. | The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment. | The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable. |
| R3.3. | LOWER | The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. | The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. | The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. | The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. |
| R4. | LOWER | The Responsible Entity did not maintain complete 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, missing at least one individual but less than 5% of the authorized personnel. | The Responsible Entity did not maintain complete 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, missing 5% or more but less than 10% of the authorized personnel. | The Responsible Entity did not maintain complete 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, missing 10% or more but less than 15%of the authorized personnel. | The Responsible Entity did not maintain complete 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, missing 15% or more of the authorized personnel. |
| R4.1. | LOWER | N/A | The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly. | The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel. | The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel. |
| R4.2. | MEDIUM | N/A | The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets. | The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause. | The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets. |

## E. Regional Variances

None identified.

### Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 01/16/06 | D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…" | 03/24/06 |
| 1 | 06/01/06 | D.2.1.4 — Change "access control rights" to "access rights." | 06/05/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Reference to emergency situations.<br>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.<br>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.<br>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".<br>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Update version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by NERC Board of Trustees | Update |
| 4 | Board approved 01/24/2011 | Update version number from "3" to "4" | Update to conform to changes to CIP-002-4 (Project 2008-06) |
| 4 | 4/19/12 | FERC Order issued approving CIP-004-4 (approval becomes effective June 25, 2012)<br><br>Added approved VRF/VSL table to section D.2. | |

| | | | |
|---|---|---|---|
| 3a - 4a | 5/24/12 | Interpretation of R2, R3, and R4 adopted by NERC Board of Trustees | |

**Appendix 1**

| **Requirement Number and Text of Requirement** |
|---|
| R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.<br><br>R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.<br><br>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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:<br><br>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. |
| **Question 1** |
| The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? |
| **Response to Question 1** |
| WECC asks three questions, which are listed below. The answer to each question follows the question.<br><br>1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4. |

2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

## A. Introduction

**1. Title:** Cyber Security — Personnel & Training

**2. Number:** CIP-004-~~4~~4a

**3. Purpose:** Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.

**4. Applicability:**

**4.1.** Within the text of Standard CIP-004-4, "Responsible Entity" shall mean:

**4.1.1** Reliability Coordinator.

**4.1.2** Balancing Authority.

**4.1.3** Interchange Authority.

**4.1.4** Transmission Service Provider.

**4.1.5** Transmission Owner.

**4.1.6** Transmission Operator.

**4.1.7** Generator Owner.

**4.1.8** Generator Operator.

**4.1.9** Load Serving Entity.

**4.1.10** NERC.

**4.1.11** Regional Entity.

**4.2.** The following are exempt from Standard CIP-004-4:

**4.2.1** Facilities regulated by the Canadian Nuclear Safety Commission.

**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.3** In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54

**4.2.4** Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.

**5. Effective Date:** The first day of the eighth calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

**R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound

security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

**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-004-4, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

**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-004-4.

**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.

## C. Measures

**M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

**M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

**M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

**M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

#### 1.2. The RE shall serve as the CEA with the following exceptions:

**1.2.1** For entities that do not work for the Regional Entity, the Regional Entity shall serve as the Compliance Enforcement Authority.

**1.2.2** For Reliability Coordinators and other functional entities that work for their Regional Entity, the ERO shall serve as the Compliance Enforcement Authority.

**1.2.3** For Responsible Entities that are also Regional Entities, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.

**1.2.4** For the ERO, a third-party monitor without vested interest in the outcome for the ERO shall serve as the Compliance Enforcement Authority.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

**1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.5. Additional Compliance Information

### 2. Violation Severity Levels

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|---|---|---|---|---|---|
| R1. | LOWER | The Responsible Entity established, implemented, and maintained but did not document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive ongoing reinforcement in sound security practices. | The Responsibility Entity did not provide security awareness reinforcement on at least a quarterly basis. | The Responsible Entity did document but did not establish, implement, nor maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. | The Responsible Entity did not establish, implement, maintain, nor document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. |
| R2. | LOWER | The Responsible Entity established, implemented, and maintained but did not document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. | The Responsibility Entity did not review the training program on an annual basis. | The Responsible Entity did document but did not establish, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. | The Responsible Entity did not establish, document, implement, nor maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. |
| R2.1. | MEDIUM | At least one individual but less than 5% of personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. | At least 5% but less than 10% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. | At least 10% but less than 15% of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. | 15% or more of all personnel having authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, were not trained prior to their being granted such access except in specified circumstances such as an emergency. |

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|---|---|---|---|---|---|
| R2.2. | MEDIUM | N/A | The training does not include one of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4. | The training does not include two of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4. | The training does not include three or more of the minimum topics as detailed in R2.2.1, R2.2.2, R2.2.3, R2.2.4. |
| R2.2.1. | LOWER | N/A | N/A | N/A | N/A |
| R2.2.2. | LOWER | N/A | N/A | N/A | N/A |
| R2.2.3. | LOWER | N/A | N/A | N/A | N/A |
| R2.2.4. | LOWER | N/A | N/A | N/A | N/A |
| R2.3. | LOWER | N/A | N/A | The Responsible Entity did maintain documentation that training is conducted at least annually, but did not include either the date the training was completed or attendance records. | The Responsible Entity did not maintain documentation that training is conducted at least annually, including the date the training was completed or attendance records. |
| R3. | MEDIUM | N/A | The Responsible Entity has a 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, but the program is not documented. | The Responsible Entity has a personnel risk assessment program as stated in R3, but conducted the personnel risk assessment pursuant to that program after such personnel were granted such access except in specified circumstances such as an emergency. | The Responsible Entity does not 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.<br><br>OR<br><br>The Responsible Entity did not conduct the personnel risk assessment pursuant to that program for personnel granted such access except in specified circumstances such as an emergency. |
| R3.1. | LOWER | N/A | N/A | The Responsible Entity did not ensure that an assessment conducted included an identity verification (e.g., Social Security Number verification in the U.S.) or a seven-year criminal check. | The Responsible Entity did not 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. |

| Requirement | VRF | Lower VSL | Moderate VSL | High VSL | Severe VSL |
|---|---|---|---|---|---|
| R3.2. | LOWER | N/A | The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment but did update it for cause when applicable. | The Responsible Entity did not update each personnel risk assessment for cause (when applicable) but did at least updated it every seven years after the initial personnel risk assessment. | The Responsible Entity did not update each personnel risk assessment at least every seven years after the initial personnel risk assessment nor was it updated for cause when applicable. |
| R3.3. | LOWER | The Responsible Entity did not document the results of personnel risk assessments for at least one individual but less than 5% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. | The Responsible Entity did not document the results of personnel risk assessments for 5% or more but less than 10% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. | The Responsible Entity did not document the results of personnel risk assessments for 10% or more but less than 15% of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. | The Responsible Entity did not document the results of personnel risk assessments for 15% or more of all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, pursuant to Standard CIP-004-4. |
| R4. | LOWER | The Responsible Entity did not maintain complete 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, missing at least one individual but less than 5% of the authorized personnel. | The Responsible Entity did not maintain complete 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, missing 5% or more but less than 10% of the authorized personnel. | The Responsible Entity did not maintain complete 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, missing 10% or more but less than 15%of the authorized personnel. | The Responsible Entity did not maintain complete 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, missing 15% or more of the authorized personnel. |
| R4.1. | LOWER | N/A | The Responsible Entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly. | The Responsible Entity did not update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel. | The Responsible Entity did not review the list(s) of all personnel who have access to Critical Cyber Assets quarterly, nor update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, nor any change in the access rights of such personnel. |
| R4.2. | MEDIUM | N/A | The Responsible Entity did not revoke access within seven calendar days for personnel who no longer require such access to Critical Cyber Assets. | The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause. | The Responsible Entity did not revoke access to Critical Cyber Assets within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer require such access to Critical Cyber Assets. |

E. **Regional Variances**

None identified.

**Version History**

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 01/16/06 | D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…" | 03/24/06 |
| 1 | 06/01/06 | D.2.1.4 — Change "access control rights" to "access rights." | 06/05/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Reference to emergency situations.<br>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.<br>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.<br>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".<br>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Update version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by NERC Board of Trustees | Update |
| 4 | Board approved 01/24/2011 | Update version number from "3" to "4" | Update to conform to changes to CIP-002-4 (Project 2008-06) |
| 4 | 4/19/12 | FERC Order issued approving CIP-004-4 (approval becomes effective June 25, 2012) | |

| | | | |
|---|---|---|---|
| | | Added approved VRF/VSL table to section D.2. | |
| 3a - 4a | 5/24/12 | Interpretation of R2, R3, and R4 adopted by NERC Board of Trustees | |

## Appendix 1

| **Requirement Number and Text of Requirement** |
|---|
| R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.<br><br>R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.<br><br>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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:<br><br>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. |
| **Question 1** |
| The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? |
| **Response to Question 1** |
| WECC asks three questions, which are listed below. The answer to each question follows the question.<br><br>1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.<br><br>Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4. |

2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

# Exhibit C

Consideration of Comments for interpretation to Requirements R2, R3, and R4 of CIP-004-4— Personnel and Training

**Project 2009-26**
**Interpretation of CIP-004-1**

Related Files

**Status:**
Adopted by the Board of Trustees on May 24, 2012, pending regulatory approval.

**Purpose / Industry Need:**
WECC requested an interpretation of CIP-004-1 Requirements R2 through R4.

| Draft | Action | Dates | Results | Consideration of Comments |
|---|---|---|---|---|
| Interpretation of CIP-004-x, Requirements R2-R4<br>Clean<br><br>**Supporting Documents**<br>CIP-004-3 | Recirculation Ballot<br><br>Info<br><br>Vote>> | 4/20/12 - 4/30/12 | Summary<br><br>Full Record | |
| **Draft 2**<br><br>Interpretation of CIP-004-x, Requirements R2-R4<br>Clean\| Redline to last posted<br><br>**Supporting Documents**<br>CIP-004-3<br>Unofficial Comment Form (Word) | Successive Ballot<br><br>Updated Info<br>Vote>><br><br>Info | 03/13/12 - 03/23/12 (closed) | Summary<br><br>Full Record | |
| | Formal Comment Period<br><br>Submit Comments >> | 02/07/12 - 03/23/12 (closed) | Comments Received | Consideration of Comments **(2)** |
| | Ballot Pool<br><br>Join>> | 02/07/12 - 03/08/12 | | |

| | | | | |
|---|---|---|---|---|
| | | (closed) | | |
| | | | | |
| WECC<br>CIP-004-1 Requirements R2-R4<br><br>Request for Interpretation<br><br>Interpretation | Initial Ballot<br><br>Vote>> \| Info | 01/06/10 - 01/19/10 (closed) | Summary<br><br>Final Results | Consideration of Comments **(1)** |
| | Pre-ballot Review<br><br>Join>> \| Info | 12/07/09 - 01/06/10 (closed) | | |
| To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice. | | | | |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Consideration of Comments

## Interpretation of CIP-004-1 by WECC (Project 2009-26)

The Interpretation of CIP-004-2 Drafting Team thanks all commenters who submitted comments on the interpretation of CIP-004-1 – Cyber Security – Personnel & Training, Requirement R2, R3, and R4, for WECC. This interpretation was posted for a 10-day initial ballot from January 6, 2010 – January 19, 2010. Stakeholders were asked to provide feedback on the interpretation and associated documents through an electronic comment system. There were 80 sets of comments, including comments from approximately 80 different people from approximately 53 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

**The Industry Segments are:**

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

| Voter | Entity | Segment |
|---|---|---|
| Rick Spyker | AltaLink Management Ltd. | 1 |
| Kirit S. Shah | Ameren Services | 1 |
| Jason Shaver | American Transmission Company, LLC | 1 |
| Donald S. Watkins | Bonneville Power Administration | 1 |
| Tony Kroskey | Brazos Electric Power Cooperative, Inc. | 1 |
| Paul Rocha | CenterPoint Energy | 1 |
| Robert Martinko | FirstEnergy Energy Delivery | 1 |
| Harold Taylor, II | Georgia Transmission Corporation | 1 |
| Ronald D. Schellberg | Idaho Power Company | 1 |
| Larry E Watt | Lakeland Electric | 1 |
| Terry Harbour | MidAmerican Energy Co. | 1 |
| John Canavan | NorthWestern Energy | 1 |
| Richard J. Kafka | Potomac Electric Power Co. | 1 |
| Kenneth D. Brown | Public Service Electric and Gas Co. | 1 |
| Tim Kelley | Sacramento Municipal Utility District | 1 |
| Robert Kondziolka | Salt River Project | 1 |
| Pawel Krupa | Seattle City Light | 1 |
| Richard Salgo | Sierra Pacific Power Co. | 1 |
| Dana Cabbell | Southern California Edison Co. | 1 |
| Horace Stephen Williamson | Southern Company Services, Inc. | 1 |
| Keith V. Carman | Tri-State G & T Association Inc. | 1 |
| John Tolo | Tucson Electric Power Co. | 1 |

| | | |
|---|---|---|
| Chuck B Manning | Electric Reliability Council of Texas, Inc. | 2 |
| Kim Warren | Independent Electricity System Operator | 2 |
| Kathleen Goodman | ISO New England, Inc. | 2 |
| Jason L Marshall | Midwest ISO, Inc. | 2 |
| Alden Briggs | New Brunswick System Operator | 2 |
| Gregory Campoli | New York Independent System Operator | 2 |
| Bobby Kerley | Alabama Power Company | 3 |
| Thomas R. Glock | Arizona Public Service Co. | 3 |
| Rebecca Berdahl | Bonneville Power Administration | 3 |
| Linda R. Jacobson | City of Farmington | 3 |
| Russell A Noble | Cowlitz County PUD | 3 |
| Jalal (John) Babik | Dominion Resources, Inc. | 3 |
| Joanne Kathleen Borrell | FirstEnergy Solutions | 3 |
| Leslie Sibert | Georgia Power Company | 3 |
| R Scott S. Barfield-McGinnis | Georgia System Operations Corporation | 3 |
| Gwen S Frazier | Gulf Power Company | 3 |
| Don Horsley | Mississippi Power | 3 |
| Terry L Baker | Platte River Power Authority | 3 |
| Jeffrey Mueller | Public Service Electric and Gas Co. | 3 |
| Kenneth R. Johnson | Public Utility District No. 1 of Chelan County | 3 |
| Greg Lange | Public Utility District No. 2 of Grant County | 3 |
| James Leigh-Kendall | Sacramento Municipal Utility District | 3 |
| John T. Underhill | Salt River Project | 3 |
| Dana Wheelock | Seattle City Light | 3 |
| Ronald L Donahey | Tampa Electric Co. | 3 |
| James R. Keller | Wisconsin Electric Power Marketing | 3 |
| Gregory J Le Grave | Wisconsin Public Service Corp. | 3 |
| David Frank Ronk | Consumers Energy | 4 |
| Guy Andrews | Georgia System Operations Corporation | 4 |
| Douglas Hohlbaugh | Ohio Edison Company | 4 |
| John D. Martinsen | Public Utility District No. 1 of Snohomish County | 4 |

| | | |
|---|---|---|
| Mike Ramirez | Sacramento Municipal Utility District | 4 |
| Hao Li | Seattle City Light | 4 |
| Anthony Jankowski | Wisconsin Energy Corp. | 4 |
| Francis J. Halpin | Bonneville Power Administration | 5 |
| Alan Gale | City of Tallahassee | 5 |
| James B Lewis | Consumers Energy | 5 |
| Mike Garton | Dominion Resources, Inc. | 5 |
| Kenneth Dresner | FirstEnergy Solutions | 5 |
| Gary L Tingley | Portland General Electric Co. | 5 |
| David Murray | PSEG Power LLC | 5 |
| Thomas J. Bradish | RRI Energy | 5 |
| Bethany Wright | Sacramento Municipal Utility District | 5 |
| Glen Reeves | Salt River Project | 5 |
| Michael J. Haynes | Seattle City Light | 5 |
| Martin Bauer | U.S. Bureau of Reclamation | 5 |
| Linda Horn | Wisconsin Electric Power Co. | 5 |
| Edward P. Cox | AEP Marketing | 6 |
| Brenda S. Anderson | Bonneville Power Administration | 6 |
| Louis S Slade | Dominion Resources, Inc. | 6 |
| Mark S Travaglianti | FirstEnergy Solutions | 6 |
| Paul Shipps | Lakeland Electric | 6 |
| James D. Hebson | PSEG Energy Resources & Trade LLC | 6 |
| Dennis Sismaet | Seattle City Light | 6 |
| William Mitchell Chamberlain | California Energy Commission | 9 |
| Jerome Murray | Oregon Public Utility Commission | 9 |
| Kent Saathoff | Electric Reliability Council of Texas, Inc. | 10 |
| Louise McCarren | Western Electricity Coordinating Council | 10 |

**Consideration of Comments on Initial Ballot — Interpretation of CIP-004-1 by WECC (Project 2009-26)**

**Summary Consideration:**
Since the previously-posted interpretation, the Interpretation Drafting Team ("IDT") has considered all of the submitted comments, and revised the interpretation. In addition to revisions made to address issues identified by commenters, the team revised the interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. Consistent with the guidance in the Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

Many commenters disagreed with the previously-posted interpretation's statement that there is no effective way to provide escorted or supervised cyber access, and they further noted that it is possible to provide escorted cyber access. Other comments note that escorted or supervised cyber access should be allowed.

The IDT recognizes there may be tools that allow escorted cyber access. However, pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT must consider the words of the standard as written. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, the standard requires that all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.

Additionally, the IDT does not believe the standard allows for escorted or supervised cyber access to cyber assets, but agrees that the standard does allow for escorted or supervised physical access to cyber assets, as explained in the revised interpretation language.

Some commenters expressed concern about limitations in emergency situations. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures.

Other commenters noted concern about the reference in the previously-posted interpretation to the FAQ document. The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an

approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access. Although WECC's Request for Interpretation was submitted on CIP-004-1, this interpretation is applicable to all subsequent versions of the standard in which the requirement language for which the interpretation was requested persists. The FAQ was written for Version 1 of the CIP standards and the language concerning authorized access has not been modified to conform to the changes made in subsequent versions.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Shrayshuen, at 404-446-2563 or at herb.shrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[2]

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Chuck B Manning | Electric Reliability Council of Texas, Inc. | 2 | Negative | "ERCOT disagrees with the statement that "there is no way to provide effective escorted or supervised cyber access". The remote terminal session capabilities (e.g.: WebEx, etc.) do provide the means for supervised or "escorted" logical access. There are many instances where an entity will have to seek support from a call center and utilize the capabilities of whoever is available for support at that time. With many of these call centers being globally located, it is not feasible to utilize a pre-determined list of support technicians who have been screened or trained as required. These support scenarios may not be of a severity for the organization to actually declare an emergency thus triggering the CIP-003-1 R3 requirement." |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language . As written, CIP-004 requires that all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |

[2] The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| David Murray | PSEG Power LLC | 5 | Affirmative | "PSEG agrees that background checks and training are appropriate those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed." |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Gary L Tingley | Portland General Electric Co. | 5 | Negative | 1. NERC needs to better define "authorized access". 2. Authorized access should not include temporary vendor support that is accomplished under the supervision of an authorized individual. |
| **Response**: Thank you for the comment. The interpretation language has been revised. The IDT also notes that any change to the standard or associated definitions, such as your comment concerning better defining "authorized access," is outside the scope of the interpretation process. Nonetheless, while the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Edward P. Cox | AEP Marketing | 6 | Negative | AEP agrees with the SDT's response to question #2 and believes that a similar response should have been provided to question #1 as well. Simply stated, as the SDT described in its first sentence, " . . . the ACE referenced in BAL-002-0 Requirement 4 is ACE as defined in BAL-001-0.1a Requirement 1 . . . " The requesting entity is seeking to have the SDT approve that their particular application of an "adjusted ACE" for the standard is compliant. AEP believes that the definition of ACE, as defined in BAL-001-0.1a R1, provides for adjustments by the ADI as a pseudo-tie falling in the Net Interchange value and by time correction falling in the Frequency Schedule value. In response to the interpretation request, the SDT introduced an equivalent "reporting ACE" term that is not contained within the referenced standard requirements. The SDT then explains the |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | use of an ACE Diversity Interchange (ADI) in the context of a Reserve Sharing Group (RSG). The use of a new term and the subsequent ADI/RSG discussion modifies the standard requirements by interpretation, which is not consistent with the use of a request for interpretation. |
| **Response**: The IDT believes that this comment was intended for a different interpretation's posting and is outside the scope of this interpretation. | | | | |
| Jason Shaver | American Transmission Company, LLC | 1 | Negative | ATC appreciates the work of the standards drafting team but disagrees with the proposed interpretation. It is our understanding that the requirements in question apply strictly to those individuals that are granted un-supervised access to a cyber asset or un-escorted physical access of a Critical Cyber Asset. We believe that there are acceptable protocols/ processes that can provide effective supervision of a person within a cyber asset and therefore disagree with the SDT opinion that ""...there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors...". If an entity has protocols/processes in regards to supervision of a person accessing a cyber asset electronically then CIP-004-1 Requirements 2, 3 and 4 would not be applicable to the person being supervised. ATC recommends the following interpretation: CIP-004-1 Requirement 2, 3 and 4 govern the actions of an entity in their dealings over persons with authorized cyber access or authorized unescorted physical access to Critical Cyber Asset(s). In so much that they grant a person un-supervised or un-escorted access to either portions of or all Critical Cyber Assets. These requirements do not apply to persons who are supervised / escorted while they are accessing a cyber asset electronically or physically. |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| concept or any words relating to “escorting” or “supervision” in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Brenda S. Anderson | Bonneville Power Administration | 6 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Donald S. Watkins | Bonneville Power Administration | 1 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Francis J. Halpin | Bonneville Power Administration | 5 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Rebecca Berdahl | Bonneville Power Administration | 3 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

**Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to “physical access,” the concept or any words relating to “escorting” or “supervision” relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of “authorized access” in the requirement does not exclude vendor support.

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. | | | | |
| Bethany Wright | Sacramento Municipal Utility District | 5 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| James Leigh-Kendall | Sacramento Municipal Utility District | 3 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Mike Ramirez | Sacramento Municipal Utility District | 4 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |
| Tim Kelley | Sacramento Municipal Utility District | 1 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. The IDT notes that this interpretation does not affect an entity's ability to fully vet a vendor pursuant to Requirements R2, R3, and R4. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures. | | | | |
| Terry Harbour | MidAmerican Energy Co. | 1 | Negative | Contrary to the interpretation, MidAmercian believes you can 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 |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | electronic access |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Kent Saathoff | Electric Reliability Council of Texas, Inc. | 10 | Negative | ERCOT disagrees with the statement that "there is no way to provide effective escorted or supervised cyber access". Remote terminal session capabilities (e.g.: WebEx, etc.) do provide the means for supervised or "escorted" logical access. There are many instances where an entity will have to seek support from a call center and utilize their capabilities. With many of these call centers being globally located, it is not feasible to utilize a pre-determined list of support technicians who have been screened or trained as required. These support scenarios may not be of a severity for the organization to actually declare an emergency thus triggering the CIP-003-1 R3 requirement. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Linda R. Jacobson | City of Farmington | 3 | Negative | FEUS thanks the drafting team for the interpretation, however, does not fully agree. FEUS SME's decided to vote No on this interpretation. The interpretation does not clarify "authorized access" as it applies to temporary support from vendors for cyber access. FEUS does not agree effective escorted or supervised cyber access cannot be accomplished in some circumstances; such as, an authorized individual working directly with temporary vendor support. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Douglas Hohlbaugh | Ohio Edison Company | 4 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |
| Joanne Kathleen Borrell | FirstEnergy Solutions | 3 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | support. |
| Kenneth Dresner | FirstEnergy Solutions | 5 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Mark S Travaglianti | FirstEnergy Solutions | 6 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |
| Robert Martinko | FirstEnergy Energy Delivery | 1 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |
| **Response**: Thank you for your comment. The IDT agrees in part and respectfully disagrees in part. In response to comments, the interpretation | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| language has been changed. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Alan Gale | City of Tallahassee | 5 | Negative | I am voting no because the standard, as written, allows a 30 day or 90 day grace period to perform the PRA and Training. This provision is removed from Version 2, both have to be performed prior to granting access. An entity could allow access to CCA's and not have the PRA/training done and be compliant if the access is for less than 30-days. While I agree it is not desired, it is allowed as written. The next version does NOT allow it. The Interpretation process cannot be used to start "enforcing" the next version prior to its authorization and implementation dates. |
| **Response**: Thank you for your comment. While the original request for interpretation was of CIP-004-1, as you have noted, the 30- and 90-day periods were eliminated in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. The drafting team agrees that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. | | | | |
| John Tolo | Tucson Electric Power Co. | 1 | Negative | I respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, I disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. I believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. I am therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." I believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. I believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the IDT disagrees that "authorized access" does not apply to vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Tony Kroskey | Brazos Electric Power Cooperative, Inc. | 1 | Negative | In one part of the response it says "there is no way to provide effective escorted or supervised cyber access" without a PRA and training to ensure that actions of the vendor do not harm. However, even with a PRA and training you still cannot ensure this. This interpretation needs more work. |
| **Response**: Thank you for your comment. The IDT has revised the interpretation in response to comments and pursuant to the NERC Guidelines for | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Interpretation Drafting Teams. | | | | |
| Richard J. Kafka | Potomac Electric Power Co. | 1 | Affirmative | Issue is "escorted access" for cyber assets. Interpretation says that there can be escorted physical access, but there is no such thing as escorted cyber access. Everyone with cyber access, including vendors, must meet the training a background checks for the registered entity's cyber security policy. As difficult as this may be for vendors and their customers, that is no reason other than emergencies to grant an exception to those who may have cyber access. |
| **Response**: Thank you for your comment. The IDT agrees, as explained in the revised interpretation. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Richard Salgo | Sierra Pacific Power Co. | 1 | Negative | It does not appear that the Drafting Team added any clarity to the term "authorized access" with this interpretation. It is our belief that "authorized access" refers to the authorization of permanent, direct, and unsupervised access to critical cyber assets, and disagree with the assertion that there is no means to provide effective supervision of vendor access to CCA's. We are troubled by the apparent dismissal of guidance provided in the FAQ's, as these FAQ's are heavily relied upon by the industry to guide compliance activities and decisions. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude temporary or non-permanent access.<br><br>The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Jalal (John) Babik | Dominion Resources, Inc. | 3 | Negative | Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability. |
| Louis S Slade | Dominion Resources, Inc. | 6 | Negative | Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability. |
| Mike Garton | Dominion Resources, Inc. | 5 | Negative | Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability. |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude support vendors. | | | | |
| Alden Briggs | New Brunswick System Operator | 2 | Negative | NBSO is voting 'no' due to the physical access issue. Pertaining to physical access, NBSO believes that a person who is escorted by someone that has authorized access (PRA and cyber training) does not need the training. Pertaining to electronic access, NBSO believes all personal that have electronic access need to be trained. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| **Response**: Thank you for your comment. The IDT agrees as explained in the revised interpretation. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| James D. Hebson | PSEG Energy Resources & Trade LLC | 6 | Affirmative | PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non-emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed. |
| Jeffrey Mueller | Public Service Electric and Gas Co. | 3 | Affirmative | PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed. |
| Kenneth D. Brown | Public Service Electric and Gas Co. | 1 | Affirmative | PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed. |
| **Response:** Thank you for your comment. The IDT agrees in part and respectfully disagrees in part. In response to comments and pursuant the NERC's Guidelines for Interpretation Drafting Teams, the interpretation language has been changed. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. The IDT notes that the scope of this interpretation does not limit an | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| entity's emergency response procedures. | | | | |
| Russell A Noble | Cowlitz County PUD | 3 | Negative | Requirement for vendors to submit to each entity's Risk Assessment and Cyber Training program appears not workable. Once an entity finds a vendor not cooperative, what then? When buying new equipment, vendors are more cooperative. But for older equipment/software there is not much incentive to induce vendors to comply. This forces the entity in a very hard position. |
| **Response**: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. | | | | |
| Dana Wheelock | Seattle City Light | 3 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Dennis Sismaet | Seattle City Light | 6 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003- |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | 1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. Thank you. |
| Hao Li | Seattle City Light | 4 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Michael J. Haynes | Seattle City Light | 5 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Pawel Krupa | Seattle City Light | 1 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Paul Shipps | Lakeland Electric | 6 | Negative | Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Larry E Watt | Lakeland Electric | 1 | Negative | supervised cyber access is possible and manageable by any able cyber security team and should not require the time and expense of training vendors for single access sessions. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Ronald L Donahey | Tampa Electric Co. | 3 | Negative | Tampa Electric thanks the Standards Drafting Team for the opportunity to comment during the Initial Ballot for the interpretation of Project 2009-26. , WECC Interpretation. We believe cyber escorting of personnel without specifically authorized access should be allowed without requiring a pre-screening via the Personnel Risk Assessment and pre-NERC training as in a network operation center support arrangement. The support vendors cannot always guarantee the availability of specific support personnel during an emergency or unplanned situation. This leaves a utility in position of potential violation versus a potential reliability issue if this is not resolved. Tampa Electric proposes that NERC establish some type of vendor certification program for the sector that would allow major systems vendors (such as Areva, GE, Emerson,Cisco, etc.) to certify at the energy sector level that they meet the Personnel Risk Assessment and training requirements so that each utility does not need to perform this for personnel who are working throughout the industry for multiple entities. It the interpretation of the drafting team as currently worded is adopted, then we suggest that the certification program be developed first so that vendors can certify to NERC that they meet the requirements which would allow them to be certified for utility purposes. It is our position that the Standards Drafting Team has not sufficiently addressed the question raised by WECC on the supervision or escorted cyber access. Based on these factors, Tampa Electric votes no to the adoption of this interpretation. |
| **Response**: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| James B Lewis | Consumers Energy | 5 | Negative | The interpretation seems to make the determination that there is “no way to provide effective escorted or supervised cyber access”. Thus, anyone granted any type of cyber access to a critical cyber asset must be compliant with CIP-004 R2, R3 and R4. Our Subject Matter Experts believe that there are acceptable protocols that can provide effective supervision of a person accessing critical cyber assets. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to “physical access,” the concept or any words relating to “escorting” or “supervision” relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Bobby Kerley | Alabama Power Company | 3 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | employee at all and this would be considered compliant. But if we don't train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |
| Don Horsley | Mississippi Power | 3 | Negative | The interpretation states "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. " We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement "...there is no way to provide...". This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don't train and |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |
| Gwen S Frazier | Gulf Power Company | 3 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don’t train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Horace Stephen Williamson | Southern Company Services, Inc. | 1 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don’t train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |
| Leslie Sibert | Georgia Power Company | 3 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement "...there is no way to provide...". This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don't train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |

**Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude temporary or non-permanent access.

The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| modified to eliminate the need for the interpretation. | | | | |
| Paul Rocha | CenterPoint Energy | 1 | Negative | The SAR Drafting team indicated the FAQ document should not be relied upon for guidance in this case. CenterPoint Energy does not agree that an interpretation should replace previously published documents intended to guide entities in their compliance efforts. The disagreement between the FAQ document and the SAR Drafting team's interpretation creates confusion and therefore CenterPoint Energy must submit a negative vote. |
| **Response**: Thank you for the comment. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Kim Warren | Independent Electricity System Operator | 2 | Negative | The scenario that WECC is concerned with presents a situation where it is quite likely that emergency support personnel would not be granted authorized access but would conduct their work using an account that has been authorized to the person who is required to escort or “supervise” the work being done under the account. The authorized owner of the account would be responsible, and in fact liable, for all activities that occur using that account. This places the onus on the account owner not the emergency support personnel which in turn places the requirement for training and PRA on the account owner not the emergency support personnel. The emergency support personnel are not being granted authorized access but are allowed the supervised use of an account that has been authorized to somebody else. NERC CIP-004-1 R2,R3 refer to authorized access as the determining factor for the requirement of training and Personnel Risk Assessment. As the situation for which WECC is seeking clarification contemplates a situation where, in all likelihood, authorized access would not be granted, therefore training and a PRA are not required. The interpretation that is presented does not contemplate this situation and therefore does not provide an |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | appropriate or complete interpretation. It is suggested that the interpretation be revised to reflect the scenario as described. |
| **Response**: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures. | | | | |
| Gregory J Le Grave | Wisconsin Public Service Corp. | 3 | Negative | The standard should allow the escorted cyber access. It is the responsibility of the entity to assure that the escorting can detect malicious behavior. Failure to implement adequate controls would be a violation of the standard. |
| **Response**: The IDT is limited by the Guidelines for Interpretation Drafting Teams to clarify the meaning of the standard, not to expand the reach of the standard. While the IDT appreciates the comment, any change of the standard is outside the scope of the interpretation process. | | | | |
| Anthony Jankowski | Wisconsin Energy Corp. | 4 | Negative | There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| James R. Keller | Wisconsin Electric Power Marketing | 3 | Negative | There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel. |
| Linda Horn | Wisconsin Electric Power Co. | 5 | Negative | There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. Local assistance from support personnel must be managed as authorized cyber access, authorized unescorted physical access, or through visitor management programs, and this interpretation does not change requirements for compliance evidence. | | | | |
| Greg Lange | Public Utility District No. 2 of Grant County | 3 | Negative | This interpretation does not answer the second part of Question one and therefore does not lend any clarity to the requested interpretation. |
| **Response**: Thank you for the comment. The interpretation language has been revised. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Guy Andrews | Georgia System Operations Corporation | 4 | Negative | We are in agreement with the following comments provided by WECC: We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | FERC. |
| Harold Taylor, II | Georgia Transmission Corporation | 1 | Negative | We are in agreement with the following comments provided by WECC: We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| David Frank Ronk | Consumers Energy | 4 | Negative | We concur with the comments provided by ATC |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Jason L Marshall | Midwest ISO, Inc. | 2 | Negative | We disagree with ignoring the FAQ that was developed by the standards drafting team. It gives insight into the intent of the SDT when developing the standard. The FAQ clearly considers cyber escorting possible. We do not think the drafting team should prevent creative solutions that may allow cyber escorting since the standard does not specifically exclude it. Further, the interpretation seems to imply that the background check must be completed prior to granting access. The standard is clear that any background checks can be completed up to 30 days after the access is granted. |
| **Response**: Thank you for the comment. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Kathleen Goodman | ISO New England, Inc. | 2 | Negative | We disagree with the interpretation, as stated. The standard does allow for escorted/ supervised access to cyber assets for both logical and physical. However, if a company allowed external logical access the individual would need to meet the standard. If the individual is physically on site and is given logical access and is supervised by a qualified escort this is allowed. Therefore, we believe the Interpretation changes the existing Standard. Further, the statement by the SDT that "It is further noted that an FAQ is not a standard, and cannot create or dilute the language of the standard itself." seems to support the argument for expansion of the requirements since the FAQs, historically, have been used extensively by the industry to develop a voting position on Standards. This Interpretation appears to change the information the industry had available to it at the time the Standard was adopted. |
| **Response**: Thank you for your comment. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| R3, and R4.<br><br>The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Kirit S. Shah | Ameren Services | 1 | Negative | We do not agrre with the interpretation. With this interpretation if a Technician from a vendor was physically escorted inside the ESP he/she would not be allowed to work on any CCA's unless he had training and background check even though he is physically escorted. This could impact operations and potentially the operation of the BES. |
| **Response**: Thank you for the comment. The interpretation language has been revised. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Dana Cabbell | Southern California Edison Co. | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Glen Reeves | Salt River Project | 5 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Gregory Campoli | New York Independent System Operator | 2 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, we disagree with the assertion that there is no way to provide effective supervision of cyber access to ensure actions do not harm the integrity of the Critical Cyber Asset or the reliability of the bulk power system. Finally, we are concerned about the reversal of previous NERC and FERC guidance. The interpretation does not directly answer the questions raised by WECC. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that is accomplished by an authorized individual working with the vendor in a supervising |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. We disagree with the assertion that there is no way to provide effective supervision of cyber access. There are tools available which can enable authorized personnel to provide temporary, indirect and monitored cyber access to personnel who have not been subjected to a personnel risk assessment and training. Furthermore, such tools can enable the supervising personnel to immediately revoke such access as needed. Therefore, we believe it is possible to provide supervised cyber access which can be controlled at least as effectively as escorted physical access. Finally, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Jerome Murray | Oregon Public Utility Commission | 9 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| John Canavan | NorthWestern Energy | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| John D. Martinsen | Public Utility District No. 1 of Snohomish County | 4 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| John T. Underhill | Salt River Project | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Keith V. Carman | Tri-State G & T Association Inc. | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| R Scott S. Barfield-McGinnis | Georgia System Operations Corporation | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Rick Spyker | AltaLink Management Ltd. | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Robert Kondziolka | Salt River Project | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Ronald D. Schellberg | Idaho Power Company | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Terry L Baker | Platte River Power Authority | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Thomas J. Bradish | RRI Energy | 5 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Thomas R. Glock | Arizona Public Service Co. | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| William Mitchell Chamberlain | California Energy Commission | 9 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Kenneth R. Johnson | Public Utility District No. 1 of Chelan County | 3 | Negative | WECC comments apply |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Louise McCarren | Western Electricity Coordinating Council | 10 | Negative | WECC respectfully disagrees with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, WECC disagrees with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. WECC believes that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. WECC is therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." WECC believes that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. WECC believes that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Martin Bauer | U.S. Bureau of Reclamation | 5 | Negative | While the SDT may have answered the questions, the response is not of the quality that can be used for reference and should be revised. There were two questions asked in this request for interpretation: 1. Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? 2. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? The response to the first question was "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." The response indicates that vendors must be authorized. Although not referenced directly it can be inferred that the response to the second questions was "....For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access....." This response is not framed well. If the inference is correct it appears to be consistent with Standard. The WECC interpretation is not consistent with the Standard. It is clear from the standards that no person can be granted permanent access and WECC is also correct that there is no standard provision for vendor temporary access except under an emergency. This does not change the response to the request for interpretation. The response is sound if it is true that there is no way to supervise cyber access as was Toni's response. "There is no such thing as escorted cyber access. I think careful reading of the standard supports that interpretation. " WECC's response in question is "We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity." |

**Response**: Thank you for the comment. The interpretation language has been revised. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3,

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| and R4. For the same reason, the scope of “authorized access” in the requirement does not exclude vendors providing temporary support. | | | | |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Consideration of Comments

## Interpretation of CIP-004-1 for Western Electricity Coordinating Council Project 2009-26

The Interpretation of CIP-004-1 for WECC Drafting Team thanks all commenters who submitted comments on the Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (Project 2009-26). These standards were posted for a parallel 45-day public comment period and intial ballot from February 7, 2012 through March 23, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 38 sets of comments, including comments from approximately 99 different people from approximately 59 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

**Summary:**

The IDT carefully reviewed all comments in response to the posting for parallel formal comment period and ballot that ended March 23, 2012. In the draft interpretation the IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. While the IDT agrees with several commenters that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term in response to WECC's request for interpretation. After considering the comments, the IDT decided not to make any changes to its interpretation, and explains its rationale in response to several minority concerns below. The interpretation is being posted for a recirculation ballot.

- One commenter does not believe that the standard separates how to treat cyber and physical access for vendors with regard to supervision. Other commenters suggest 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, the IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. Furthermore, there are a number of contexts in which

someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).

- The IDT notes that the standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.
- Several commenters provided suggestions or comments that the drafting team was not able to address and stay within the Guidelines for Interpretation Drafting Teams, and the IDT recommends that commenters provide specific comments to address these issues when the Version 5 CIP standards are posted for comment.
- Several commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES. Furthermore, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams.
- Some commenters suggested that the absence of language regarding supervision or escorting with respect to electronic access does not absolutely prohibit the concept. In response, the IDT notes the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Commenters also suggest that the standards should be modified to allow for vendor or contractor access without having to satisfy the authorization requirements. However, modification of the standard is outside the scope of an interpretation. The IDT believes that the interpretation adequately addresses that all cyber access is contemplated by the interpretation, which includes both employees and vendors.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

## Index to Questions, Comments, and Responses

**The Industry Segments are:**

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1. | Group | Guy Zito | Northeast Power Coordinating Council | | | | | | | | | | X |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Alan Adamson | New York State Reliability Council, LLC | NPCC | 10 |
| 2. | Greg Campoli | New York Independent System Operator | NPCC | 2 |
| 3. | Sylvain Clermont | Hydro-Quebec TransEnergie | NPCC | 1 |
| 4. | Chris de Graffenried | Consolidated Edison Co. of New York, Inc. | NPCC | 1 |
| 5. | Gerry Dunbar | Northeast Power Coordinating Council | NPCC | 10 |
| 6. | Mike Garton | Dominion Resources Services, Inc. | NPCC | 5 |
| 7. | Kathleen Goodman | ISO - New England | NPCC | 2 |
| 8. | Chantel Haswell | FPL Group, Inc. | NPCC | 5 |
| 9. | David Kiguel | Hydro One Networks Inc. | NPCC | 1 |
| 10. | Michael R. Lombardi | Northeast Utilities | NPCC | 1 |

| Group/Individual | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

| | | | | |
|---|---|---|---|---|
| 11. | Randy MacDonald | New Brunswick Power Transmission | NPCC | 9 |
| 12. | Bruce Metruck | New York Power Authority | NPCC | 6 |
| 13. | Lee Pedowicz | Northeast Power Coordinating Council | NPCC | 10 |
| 14. | Robert Pellegrini | The United Illuminating Company | NPCC | 1 |
| 15. | Si-Truc Phan | Hydro-Quebec TransEnergie | NPCC | 1 |
| 16. | David Ramkalawan | Ontario Power Generation, Inc. | NPCC | 5 |
| 17. | Brian Robinson | Utility Services | NPCC | 8 |
| 18. | Saurabh Saksena | National Grid | NPCC | 1 |
| 19. | Michael Schiavone | National Grid | NPCC | 1 |
| 20. | Wayne Sipperly | New York Power Authority | NPCC | 5 |
| 21. | Tina Teng | Independent Electricity System Operator | NPCC | 2 |
| 22. | Donald Weaver | New Brunswick System Operator | NPCC | 2 |
| 23. | Ben Wu | Orange and Rockland Utilities | NPCC | 1 |
| 24. | Peter Yost | Consolidated Edison Co. of New York, Inc. | NPCC | 3 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2. | Group | Emily Pennel | Southwest Power Pool Regional Entity | | | | | | | | | | | X |

No additional members listed.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3. | Group | Chris Higgins | Bonneville Power Administration | X | | X | | X | X | | | | |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Forrest | Krigbaum | WECC | 1 |
| 2. | Nick | Choi | WECC | 1 |
| 3. | Mike | Miller | WECC | 1 |
| 4. | Erika | Doot | WECC | 3, 5, 6 |
| 5. | Stephen | Larson | WECC | 1, 3, 5, 6 |
| 6. | Peter | Raschio | WECC | 1 |
| 7. | Mark | Tucker | WECC | 1, 3, 5, 6 |
| 8. | Tedd | Snodgrass | WECC | 1 |
| 9. | Huy | Ngo | WECC | 1 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4. | Group | Connie Lowe | Dominion | X | | X | | X | X | | | | |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Greg Dodson | | SERC | 1, 3, 5, 6 |
| 2. | Mike Garton | | NPCC | 5, 6 |

| Group/Individual | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3. Louis Slade | | RFC | 5, 6 | | | | | | | | | |
| 4. Michael Gildea | | MRO | 5, 6 | | | | | | | | | |
| 5. Group | David Thorne | Pepco Holdings Inc & Affiliates | X | | X | | | | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Michael | O'Grady | RFC | 1 | | | | | | | | | |
| 6. Group | Sam Ciccone | FirstEnergy | X | | X | X | X | X | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Troy Rhoades | FE | RFC | | | | | | | | | | |
| 2. M.J. Linn | FE | RFC | | | | | | | | | | |
| 3. Dough Hohlbaugh | FE | RFC | | | | | | | | | | |
| 7. Group | Dean Larson | Kansas City Power & Light | X | | X | | X | X | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Scott Harris | Kansas City Power & Light | SPP | 1, 3, 5, 6 | | | | | | | | | |
| 2. Michael Gammon | Kansas City Power & Light | SPP | 1, 3, 5, 6 | | | | | | | | | |
| 8. Group | Gregory Campoli | ISO/RTO Standards Review Committee | | X | | | | | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Albert DiCaprio | PJM | RFC | 2 | | | | | | | | | |
| 2. Mark Thompson | AESO | WECC | 2 | | | | | | | | | |
| 3. Gary DeShazo | CAISO | WECC | 2 | | | | | | | | | |
| 4. Steven Myers | ERCOT | ERCOT | 2 | | | | | | | | | |
| 5. Ben Li | IESO | NPCC | 2 | | | | | | | | | |
| 6. Matt Goldberg | ISO-NE | NPCC | 2 | | | | | | | | | |
| 7. Bill Phillips | MISO | RFC | 2 | | | | | | | | | |
| 8. Donald Weaver | NBSO | NPCC | 2 | | | | | | | | | |
| 9. Charles Yeung | SPP | SPP | 2 | | | | | | | | | |
| 9. Group | Jason Marshall | ACES Power Marketing Collaborators | | | | | | X | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. James Jones | AEPCO/SWTC | WECC | 1, 4, 5 | | | | | | | | | |
| 2. Shari Heino | Brazo Electric Power Cooperative | ERCOT | 1 | | | | | | | | | |
| 3. Michael Brytowski | Great River Energy | MRO | 1, 3, 5, 6 | | | | | | | | | |

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 4. | Bob Solomon | Hoosier Energy | RFC 1 | | | | | | | | | | |
| 10. | Group | Marie Knox | MISO Standards Collaborators | | X | | | | | | X | | |
| | **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. | Jim Cyrulewski | JDRJC Associates, LLC | RFC | 8 | | | | | | | | | |
| 11. | Group | Jesus Sammy Alcaraz | Imperial Irrigation District (IID) | X | | X | X | X | X | | | | |
| | **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. | Marcela Caballero | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 2. | Israel Gonzalez | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 3. | Peter Nguyen | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 4. | Mauricio Lopez | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 12. | Individual | Sandra Shaffer | PacifiCorp | X | | X | | X | X | | | | |
| 13. | Individual | Shane Eaker | Southern Company | X | | X | | X | X | | | | |
| 14. | Individual | Kieth Morisette | Tacoma Public Utilities | X | | X | X | X | X | | | | |
| 15. | Individual | Keira Kazmerski | Xcel Energy | X | | X | | X | X | | | | |
| 16. | Individual | Jay Walker | NIPSCO | X | | X | | X | X | | | | |
| 17. | Individual | Ronnie Hoeinghaus | City of Garland | | | X | | | | | | | |
| 18. | Individual | Andrew Z. Pusztai | American Transmission Company, LLC | X | | | | | | | | | |
| 19. | Individual | Thad Ness | American Electric Power | X | | X | | X | X | | | | |
| 20. | Individual | Randi Nyholm | Minnesota Power | X | | X | | X | X | | | | |
| 21. | Individual | Greg Rowland | Duke Energy | X | | X | | X | X | | | | |
| 22. | Individual | Brian J Murphy | NextEra Energy Inc. | X | | X | | X | X | | | | |
| 23. | Individual | Michelle R D'Antuono | Ingleside Cogeneration LP | | | | | X | | | | | |
| 24. | Individual | Michael Falvo | Independent Electricity System Operator | | X | | | | | | | | |
| 25. | Individual | Kim Koster | MidAmerican Energy Company | X | | X | | X | X | | | | |
| 26. | Individual | Kirit Shah | Ameren | X | | X | | X | X | | | | |
| 27. | Individual | Jonathan Appelbaum | United Illuminating Company | X | | | | | | | | | |
| 28. | Individual | Jim Eckelkamp | Progress Energy | X | | X | | X | X | | | | |

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 29. | Individual | Andrew Ginter | Waterfall Security Solutions | | | | | | | | X | | |
| 30. | Individual | Thomas Johnson | Salt River Project | X | | X | | X | X | | | | |
| 31. | Individual | Andrew Gallo | Austin Energy | X | | X | X | X | X | | | | |
| 32. | Individual | Patrick Brown | Essential Power, LLC | X | | | | X | | | | | |
| 33. | Individual | John Seelke | PSEG (Public Service Enterprise Group) | X | | X | | X | X | | | | |
| 34. | Individual | Christina Bigelow | Midwest ISO | | X | | | | | | | | |
| 35. | Individual | Ron Donahey | Tampa Electric Company | X | | X | | X | X | | | | |
| 36. | Individual | Joe Doetzl | CRSI | X | | | | | | | | | |
| 37. | Individual | Darryl Curtis | Oncor Electric Delivery Company | X | | | | | | | | | |
| 38. | Individual | DANA SHOWALTER | E.ON CLIMATE & RENEWABLES | | | | | X | | | | | |

1. **The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on how a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?**

**Summary Consideration:**

Most commenters agreed with the IDT that the request for interpretation asks for clarity on the meaning of a requirement. There were a few commenters that believe the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.

Some commenters suggested that the interpretation may cause difficulty in providing authorized access to vendors or contractors. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement andthe IDT must interpret a requirement according to the Guidelines for Interpretation Drafting Teams. The requirement language addresses "electronic access," and all electronic access must be authorized. Thus, regardless of a particular vendor's personnel screening or security training, any electronic access by that vendor's personnel, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The commenters also suggested that the issue should be addressed in conjunction with the CIP Version 5 development. The IDT notes that Project 2008-06 is working on Version 5 of the CIP standards, which is outside the scope of the IDT, and requests that commenters who suggested that the issue be addressed in Version 5 of the CIP standards provide specific suggestions when those standards are posted for comment.

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Midwest ISO | The request is asking for clarity on the meaning of | The request seeks clarification of the meaning of "authorized access." As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof. |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | a requirement. | |
| **Response: The IDT agrees that the request for interpretation asks for clarification on the meaning of a requirement.** | | |
| Ingleside Cogeneration LP | The request is asking for clarity on the meaning of a requirement. | WECC has requested a clarification of the definition of "authorized access" to determine if vendor personnel who provide supervised temporary support to Responsible Entities, are subject to CIP-004 R2 through R4. This is a subject of great relevance to Ingleside Cogeneration LP as we require all of our vendors to maintain robust cyber security programs, but agree with WECC that a literal reading of CIP-004 may require dedicated agents from each. Critical vendors such as Cisco or GE do not support an operating model like this - and we would argue that their security training and personnel screening procedures are superior. This subject will become especially prevalent when CIP Version 5 takes effect and all Responsible Entities will be required to have a cyber policy that addresses Cyber System Access. We would like to see this complex issue addressed now, before some precedence is set that proves to be uneconomical or unviable. |
| **Response: Thank you for your comment. The IDT must interpret a requirement according to the Guidelines for Interpretation Drafting Teams. The requirement language addresses "electronic access," and all electronic access must be authorized. Thus, regardless of a particular vendor's personnel screening or security training, any electronic access by that vendor's personnel, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT notes that Project 2008-06 is working on Version 5 of the CIP standards, which is outside the scope of the IDT. Therefore, the IDT recommends that the commentor provide specific suggestions to the Project 2008-06 SDT when the Version 5 CIP standards are posted for comment.** | | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| NextEra Energy Inc. | The request is asking for clarity on the application of a requirement. | Each of the three questions is asking whether a class of individuals (i.e., temporary vendors and supervisors of vendors) is required to comply with CIP-004 R2, R3 and R4. Thus, the questions are requesting specific confirmation whether one is or is out of compliance based on how these classes of individuals are addressed under CIP-004. |
| **Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement.** | | |
| Southwest Power Pool Regional Entity | The request is asking for clarity on the application of a requirement. | The clarification requested by WECC specifically states that the WECC RC seeks clarification on the definition of authorized access "as applied to temporary support from vendors." |
| **Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.** | | |
| MidAmerican Energy Company | The request is asking for clarity on the application of a requirement. | The request is asking for clarification on the application of the term “authorized access” in order to determine how to comply in the situation of temporary vendor support. |
| **Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement. The IDT** | | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| **believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.** | | |
| Northeast Power Coordinating Council | The request is asking for clarity on the meaning of a requirement. | |
| Dominion | The request is asking for clarity on the meaning of a requirement. | |
| FirstEnergy | The request is asking for clarity on the meaning of a requirement. | |
| ISO/RTO Standards Review Committee | The request is asking for clarity on the meaning of a requirement. | |
| ACES Power Marketing Collaborators | The request is asking for clarity on the meaning of a requirement. | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Imperial Irrigation District (IID) | The request is asking for clarity on the meaning of a requirement. | |
| NIPSCO | The request is asking for clarity on the meaning of a requirement. | |
| American Transmission Company, LLC | The request is asking for clarity on the meaning of a requirement. | |
| American Electric Power | The request is asking for clarity on the meaning of a requirement. | |
| Minnesota Power | The request is asking for clarity on the meaning of a requirement. | |
| Duke Energy | The request is asking for clarity | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | on the meaning of a requirement. | |
| Ameren | The request is asking for clarity on the meaning of a requirement. | |
| United Illuminating Company | The request is asking for clarity on the meaning of a requirement. | |
| Progress Energy | The request is asking for clarity on the meaning of a requirement. | |
| Waterfall Security Solutions | The request is asking for clarity on the meaning of a requirement. | |
| Salt River Project | The request is asking for clarity on the meaning of a requirement. | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Essential Power, LLC | The request is asking for clarity on the meaning of a requirement. | |
| PSEG (Public Service Enterprise Group) | The request is asking for clarity on the meaning of a requirement. | |
| Tampa Electric Company | The request is asking for clarity on the meaning of a requirement. | |
| CRSI | The request is asking for clarity on the meaning of a requirement. | |
| Oncor Electric Delivery Company | The request is asking for clarity on the meaning of a requirement. | |
| E.ON CLIMATE & RENEWABLES | The request is asking for clarity | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | on the meaning of a requirement. | |
| Bonneville Power Administration | The request is asking for clarity on the application of a requirement. | |
| Pepco Holdings Inc & Affiliates | The request is asking for clarity on the application of a requirement. | |
| Kansas City Power & Light | The request is asking for clarity on the application of a requirement. | |
| MISO Standards Collaborators | The request is asking for clarity on the application of a requirement. | |
| PacifiCorp | The request is asking for clarity on the application of a requirement. | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Southern Company | The request is asking for clarity on the application of a requirement. | |
| Tacoma Public Utilities | The request is asking for clarity on the application of a requirement. | |
| Xcel Energy | The request is asking for clarity on the application of a requirement. | |
| City of Garland | The request is asking for clarity on the application of a requirement. | |
| Independent Electricity System Operator | The request is asking for clarity on the application of a requirement. | |
| Austin Energy | The request is asking for clarity | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | on the application of a requirement. | |
| **Response: Thank you for your comments.** | | |

**2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?**

**Summary Consideration:**

Most commenters agree with the IDT that the interpretation does not expand the reach of the requirement, and one commenter expressed rationale that supports the IDT's interpretation by noting that allowing for the concept of supervised electronic access would expand the reach of the requirement.

One commenter believes that the interpretation expands the reach of the requirement because it uses references to standards that are not part of the standard being interpreted. The commenter suggests that such a reference would set an unacceptable precedent. In response to that concern, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors. That commenter also suggests that the interpretation reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is for physical access. However, the IDT notes that the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.

Some commenters do not believe the interpretation allows for emergency access when needed, or that the interpretation will make getting support from contractors difficult. The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.

Commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES.

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Omaha Public Power District | Negative | 1. The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement? 0 The request is asking for clarity on the meaning of a requirement. 1 The request is asking for clarity on the application of a requirement. Comments: N/A 2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard? 1 The interpretation expands the reach of the standard. 0 The interpretation does not expand the reach of the standard. Comments: OPPD respectfully disagrees with the proposed interpretation provided by NERC in response to questions submitted by WECC. Utilizing standards that are not in direct relation to the question being proposed contains no true definition or answer. This type of response sets an unacceptable precedence of using different standards and requirements to justify an interpretation. 3. Do you agree with this interpretation? If not, please explain specifically what you disagree with. 0 Yes 1 No Comments: In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | | Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, OPPD does not believe the interpretation allows for emergent electronic access when needed. OPPD believes there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, OPPD feels the risk level to the BES, in terms of reliability, is indeed increased. |
| **Response: -In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.**<br>**-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br>**-The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.** | | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| -Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. | | |
| Bonneville Power Administration | The interpretation does not expand the reach of the standard. | BPA believes that if the drafting team allowed for the concept of supervised cyber access, they would be expanding the scope CIP-004. |
| Response: Thank you for the comment and supporting rationale that reinforces the IDT's interpretation. | | |
| Northeast Power Coordinating Council | The interpretation does not expand the reach of the standard. | |
| Southwest Power Pool Regional Entity | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Pepco Holdings Inc & Affiliates | The interpretation does not expand the reach of the standard. | |
| FirstEnergy | The interpretation does not expand the reach of the standard. | |
| Kansas City Power & Light | The interpretation does not expand the reach of the standard. | |
| ISO/RTO Standards Review Committee | The interpretation does not | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | expand the reach of the standard. | |
| Imperial Irrigation District (IID) | The interpretation does not expand the reach of the standard. | |
| PacifiCorp | The interpretation does not expand the reach of the standard. | |
| Tacoma Public Utilities | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Xcel Energy | The interpretation does not expand the reach of the standard. | |
| NIPSCO | The interpretation does not expand the reach of the standard. | |
| American Transmission Company, LLC | The interpretation does not expand the reach of the standard. | |
| American Electric Power | The interpretation does not | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | expand the reach of the standard. | |
| Minnesota Power | The interpretation does not expand the reach of the standard. | |
| Duke Energy | The interpretation does not expand the reach of the standard. | |
| Independent Electricity System Operator | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Waterfall Security Solutions | The interpretation does not expand the reach of the standard. | |
| Salt River Project | The interpretation does not expand the reach of the standard. | |
| Austin Energy | The interpretation does not expand the reach of the standard. | |
| Essential Power, LLC | The interpretation does not | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | expand the reach of the standard. | |
| PSEG (Public Service Enterprise Group) | The interpretation does not expand the reach of the standard. | |
| Tampa Electric Company | The interpretation does not expand the reach of the standard. | |
| CRSI | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Oncor Electric Delivery Company | The interpretation does not expand the reach of the standard. | |
| E.ON CLIMATE & RENEWABLES | The interpretation does not expand the reach of the standard. | |
| MISO Standards Collaborators | The interpretation expands the reach of the standard. | |
| Southern Company | The interpretation expands the reach of the | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | standard. | |
| Ameren | The interpretation expands the reach of the standard. | |
| United Illuminating Company | The interpretation expands the reach of the standard. | |
| Progress Energy | The interpretation expands the reach of the standard. | |
| **Response: Thank you for your comments.** | | |

**3. Do you agree with this interpretation? If not, please explain specifically what you disagree with.**

**Summary Consideration:**

The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation. After considering the comments, the IDT decided not to make any changes to its interpretation, and explains its rationale in response to the concerns raised by commenters below.

One commenter does not believe that the standard separates how to treat cyber and physical access for vendors with regard to supervision, but the IDT notes that the standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.

Some commenters noted that training alone will not prevent a vendor from perpetrating malicious activity. In response, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and this is not supported by the language in the requirement. The standard language (and the interpretation) does not prevent supervised access; however, all electronic access must be authorized pursuant to the requirements in CIP-004. Modification of the standard to allow such electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.

Another commenter agreed with the interpretation while noting that the interpretation may confirm a logistical problem in getting vendor support when a vendor will not submit to the entity's background checks and training. This is a point that the IDT addressed in development discussions, and it determined that it is outside the scope of an interpretation. The greater standards development process is better equipped to weigh those concerns, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT understands that the Version 5 CIP SDT is aware of this logistics concern. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.

A commenter supported the IDT's rationale by noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent harm, and that granting direct cyber access inhibits that ability.

A commenter in agreement with the overall interpretation suggested that the reference to "authorized access" might be made clearer if, rather than referencing R2, R3, and R4, the interpretation specifically stated what those requirements are. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as

requested by the request for interpretation. The IDT also considered the approach of fully stating the requirements, but notes that upon approval, this interpretation will be appended to the standard itself, and R2, R3, and R4 will be easy to reference.

Several commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES. Furthermore, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams.

Commenters suggested that the absence of language regarding supervision or escorting with respect to electronic access does not absolutely prohibit the concept. In response, the IDT notes the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Some commenters also suggest that the standards should be modified to allow for vendor or contractor access without having to satisfy the authorization requirements. However, modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT believes that the interpretation adequately addresses that all cyber access is contemplated by the interpretation, which includes both employees and vendors.

Commenters suggest that the intent of the standard was to allow supervised/escorted cyber access. The IDT does not find support in the language of the standard that "the intent of the standard is to allow for supervised/escorted access for both physical and cyber access." Additionally, some commenters believe the interpretation does not allow for necessary emergency access, or that the interpretation will make getting support from contractors difficult. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements.

Commenters suggest that the interpretation defines or puts bounds on the definitions of "authorized access", "cyber access", and "physical access" and that the interpretation equates "authorized access" with being on the list under CIP-004-1, Requirement R4. The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed.

Other commenters suggest 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, the IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. Furthermore, there are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).

Commenters suggest that if a Responsible Entity can demonstrate that they can supervise remote cyber access, then that access should be allowed. The IDT believes that the relevant question to resolve is not whether an entity can supervise remote cyber access, but whether such access is allowed by the standard. The requirement language addresses "electronic access," and all electronic access must be authorized.

Commenters suggest that since "authorized access" is not in the standard, use of the phrase in the interpretation expands the reach of the standard. In response, the IDT notes that it sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.

Some commenters noted concern that the interpretation's reference of other standards sets a bad precedent, but the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.

One commenter agrees with the conclusion of the interpretation, but believes that the request for interpretation is asking for compliance guidance and that the interpretation only restates information in the standard. While the IDT agrees that the interpretation has compliance application implications, on balance, the IDT and most commenters agree that the interpretation is validly asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| Alberta Electric System Operator | Abstain | The AESO agrees with the interpretation of CIP-004, however we are casting an abstain vote as this standard is not applicable in Alberta at this time. |
| **Response: Thank you for the comment.** | | |
| Consolidated Edison Co. of New York | Affirmative | See NPCC region-wide group comment form |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: See NPCC response** | | |
| California ISO | Affirmative | Comments form provided jointly with ISO/RTO Standards Review Committee |
| **Response: See ISO/RTO response** | | |
| Electric Reliability Council of Texas, Inc. | Affirmative | ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee. |
| **Response: See ISO/RTO response** | | |
| Midwest ISO, Inc. | Affirmative | We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access. |
| **Response:**<br>"We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision."<br>**The standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.**<br>"The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity."<br>**Whether temporary or permanent, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br>"Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access." | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **The IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and this is not supported by the language in the requirement. The standard language (and the interpretation) does not prevent supervised access; however, all electronic access must be authorized pursuant to the requirements in CIP-004. Modification of the standard to allow such electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Cowlitz County PUD | Affirmative | The interpretation is correct. However it does confirm a logistical problem: how to obtain vendor support when the vendor will not submit to the entity's requirement for background checks and training. If the cyber system is broken and can only be fixed via vendor support, the time to get an Exception approved or replace the cyber asset could have a serious negative impact on the BES. |
| **Response: Thank you for the comment. This is a point that the IDT addressed in development discussions, and it determined that it is outside the scope of an interpretation. The greater standards development process is better equipped to weigh those concerns, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT understands that the Version 5 SDT is aware of this logistics concern. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.** | | |
| Wisconsin Energy Corp. | Affirmative | Comments are requested to be submitted using the separate electronic comment form rather than with the vote. While the answer gets a bit circular, and there is room for disagreement in the industry on the interpretation, I support it and do not have any specific comments to submit with this vote. |
| **Response: Thank you for your comment.** | | |
| Southwest Power Pool Regional Entity | Yes | The SPP RE agrees with the interpretation, noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent the escorted individual from overtly, covertly, or inadvertently causing harm. Granting direct cyber access to someone without authorized access inhibits the ability to perform |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | the escort responsibilities and introduces risk. As noted in the interpretation, this is why the standard specifically makes a distinction regarding "authorized, unescorted" physical access. Technically, escorted cyber access is not feasible. The SPP RE agrees that "over the shoulder" viewing via a webinar or close proximity presence, while possibly subject to the entity's CIP-003/R5 information protection program, does not constitute cyber access. |
| **Response: Thank you for the comments and rationale, which supports the IDT's interpretation.** | | |
| Tacoma Public Utilities | Yes | Agree with the standard as written in the WECC position paper |
| **Response: Thank you for the comment.** | | |
| American Electric Power | Yes | AEP agrees with the overall interpretation, but offers the following commentsand recommendations for improving the interpretation.Responses to Questions 1 and 2:The response provided for Q1 does not definitively answer the question that was posed. The question posed asks what the definition is for "authorized access", while the response essentially states that one has this access by being on the proper list. It is not clear from the response how those on the authorized list were added to it, i.e. that those individuals met the necessary training, risk assessment, and access requirements. This might be made clearer if, rather than generally mentioning R2, R3, and R4, specifically stating what those requirements are.The response provided for Question 2 more adequately addresses Question 1 than does the response to Q1. |
| **Response: Thank you for your comments. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as requested by the request for interpretation. The IDT also considered the approach of fully stating the requirements, but notes that upon approval, this interpretation will be appended to the standard itself, and R2, R3, and R4 will be easy to reference.** | | |
| PSEG (Public Service Enterprise Group) | Yes | The inability to provide Escorted Cyber Access through a web-conference (or otherwise), can be detrimental to the reliability of the BES as the time to |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | troubleshoot cyber/networking issues can be extensive without letting the remote support personnel have access to the troubled device. |
| **Response: Thank you for your comment. The IDT understands this concern, but notes that the greater standards development process is better equipped to review such a concept, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Additionally, given the provisions for emergency access and the ability to plan in advance for authorizing access, the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| Tampa Electric Company | Yes | Although we believe that the Interpretations Drafting Team has correctly provided the interpretation, we believe that the standard should be changed to provide a vehicle for emergency vendor access via cyber or physical escorting. The lack of the ability to provide this emergency access could be detrimental to the reliability of the grid and may force Entities into non-compliance to meet the emergency situation. |
| **Response: -Thank you for your comments. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to BES reliability. Considering those provisions for emergency and planned access, the IDT does not believe this interpretation is detrimental to reliability.**<br>**-The IDT notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.** | | |
| Oncor Electric Delivery Company | Yes | Oncor Electric Delivery agrees with this interpretation. The interpretation provides greater clarity on how a Compliance Enforcement Agency (CEA) addresses "cyber access" which includes both physical and remote acc |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: Thank you for your comments** | | |
| Dominion | The interpretation expands the reach of the standard. | The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard. |
| **Response: The requirement language addresses “electronic access,” and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of “escorted” supervision for individuals with electronic access, it does not include a provision for “escorted” cyber access. Thus, any electronic access, whether “escorted” or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| ACES Power Marketing Collaborators | The interpretation expands the reach of the standard. | Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines “authorized access’ by stating that an individual has “authorized access” if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated “authorized access” with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since Console access is almost always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device. |
| **Response: The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. There are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).** | | |
| NextEra Energy Inc. | The interpretation expands the reach of the standard. | It could be viewed that the interpretation requested tends to expand the reach of CIP-004, given the lack of clarity in the answers. Thus, if this interpretation goes forward, it is recommended that that the following clearer and more to the point answers be substituted for the current answers, so there is no expanding of CIP-004 nor an elaboration on how the standard applies to particular facts:1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors. Answer: The term authorized access as used in CIP-004 is not limited or qualified by any type or class of employees or vendors. Thus, all employees and vendors (who desire either physical or cyber access) without regard to whether they are temporary support or not must either: (1) be escorted by someone with authorized unescorted physical or authorized cyber access, as applicable or (2) have been granted authorized unescorted physical or authorized cyber access by meeting the requirements of R2 and R3. Thus, there is no exception for temporary support from vendors, and the term authorized access applies to them in the same manner it applies to any other class or type of employee or vendor. 2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?Answer: Yes. The language of CIP-004 applies to all employees and vendors that desire |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | unescorted physical or cyber access to Critical Cyber Assets without regard to whether or not the employee or vendor is supervised. 3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? Answer. See answer to question 2 - supervised vendors are not exempt from CIP-004-1, Requirements R2, R3, and R4, thus the remainder of the question is moot. |
| **Response: The IDT considered these suggestions. The IDT believes that the interpretation adequately addresses that *all* cyber access is contemplated by the interpretation, which includes both employees and vendors. The IDT does not fully agree with the suggested phrase, "be escorted by someone with authorized unescorted physical or authorized cyber access" with respect to CIP-004, versions 2 through 4, and believes that it only exists in version 1 with respect to the 30 and 90 day periods acknowledged in the interpretation's footnote.** | | |
| Ingleside Cogeneration LP | The interpretation expands the reach of the standard. | The project team has chosen to differentiate between escorted physical access where a vendor performs a non-cyber activity (such as replacing parts) from one where a cyber connection has been made. Ingleside Cogeneration LP believes the project team has read in extra language into the requirement - and changed FERC's intent in Order 706 paragraph 432. That paragraph was cited by WECC in the original Request for Interpretation, and clearly acknowledges that supervised access is a real-life operational need under certain circumstances. If anything, the Commission brings up a good point about the qualifications of the escort, but it does not seem appropriate that the drafting team has completely ruled out supervised cyber access. Furthermore, by logical inference, if the Responsible Entity can demonstrate that they can supervise remote cyber access, then that should be allowed as well. |
| **Response: The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT is interpreting the standard language as approved by FERC, and its interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** | | |
| MidAmerican Energy Company | The interpretation expands the reach of the standard. | WECC is seeking "clarification on the definition of 'authorized access.'" |
| **Response: Thank you for your comments. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as requested by the request for interpretation.** | | |
| Midwest ISO | The interpretation expands the reach of the standard. | MISO respectfully submits that, based on a literal reading of the plain language of CIP-004, the phrase "authorized access" is not part of the language of the requirement requested for interpretation. The use of a specific term not utilized in the requirement as well as the assignment of a specific meaning and obligations from the requirement at issue to such a term by the Interpretation Drafting Team ("IDT") in its Interpretation expands the reach of the standard. |
| **Response: The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.** | | |
| Pacific Gas and Electric Company | Negative | PG&E disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or on-site cyber access). Registered entities should be allowed to provide vendors, which they have engaged, with temporary digitally escorted access. Prohibiting this capability directly affects the safe and reliable operations of the Bulk |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | Electric System. If this interpretation is approved as worded, a valuable support tool could place utilities in a position where reliability suffers to maintain compliance. Let's take one of the well know router companies for example. This company has one of the highest performing Tier 1 support record of any company. When you call their support you reach their Tier 1 support desk which if allowed to be escorted digitally can address most issues within a reasonable timeframe. If escorted digital access is prohibited entities would have to negotiate dedicated Cisco technicians to support their devices. Not only would this be extremely costly, if possible, most importantly it would not be efficient resulting in delays to address the issue at hand. For remote access, technologies such as WebEx, TightVNC, Timbuk2, etc enable strict remote control solutions, this allows someone to provide logical remote control to a system while fully recording and visually observe (e.g., digitally escort) all actions. At any time, the escort observes anything inappropriate they can shut-off access immediately by a click of a button. In reality, allowing, "digital escorting" is much safer than allowing someone physical access to critical assets as the escort can stop any action with a click of a button whereas with physical access the "escort" has to have the capability to physically stop the individual. For on-site cyber access entities should be able to perform these activities in the same manner that they provide escorting to other visitors, through visual observation. Someone with escorted physical access can do more physical damage to critical assets faster than they can do damage typing on a keyboard with an escort observing them. For example, if the escort observes anything inappropriate being typed they can physically interrupt the individual and keep them from hitting the "enter/execute" command; however, someone can grab a handful of fiber cables going into a patch panel and yank them out before an escort could stop them. |
| **Response: The IDT does not find support in the language of the standard that "the intent of the standard is to allow for supervised/escorted access for both physical and cyber access." The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to BES reliability or safety.** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Considering those provisions for emergency and planned access, the IDT does not believe this interpretation is detrimental to reliability. The IDT also notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 standards are posted for comment.** | | |
| Salt River Project | Negative | The interpretation does not clearly define that escorted electronic access is prohibited. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| Brazos Electric Power Cooperative, Inc. | Negative | See comments provided by ACES Power Marketing. |
| **Response: See ACES response** | | |
| Southwest Transmission Cooperative, Inc. | Negative | Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines "authorized access' by stating that an individual has "authorized access" if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated "authorized access" with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | Console access is almost always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device. This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | to the interpretation, most (probably all) registered entities have a formal process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed. We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert,software expert). |
| **Response: -The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted"** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. There are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).**<br><br>**-The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. The IDT is interpreting the standard language as approved by FERC, and its interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."**<br><br>**-Modification of the standard to allow electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. However, the CIP IDT encourages the commenter to provide specific suggestions to address this issue when the Version 5 CIP standards are posted for comment.** | | |
| Central Lincoln PUD | Negative | The interpretation effectively disallows vendor cyber access, since vendors will be unwilling to undergo training established by each of their customers. The resulting lack of support will add risk to the BES. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| City and County of San Francisco | Negative | While in theory we believe the interpretation makes sense, its real world application is likely to result in undesirable consequences with respect to vendor support of control system maintenance, and have a negative impact on BES reliability. We believe that the concept of requiring a responsible Entity to have document that its vendor has personnel risk assessment program and cyber security training may be |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | worth exploring. |
| **Response: -The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.** | | |
| Essential Power, LLC | Negative | Comments: In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation. In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support. Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard. There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.** | | |
| Salt River Project | Negative | As written the interpretation does not clearly define that escorted electronic access is prohibited. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| U.S. Army Corps of Engineers | Negative | In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, we do not believe the interpretation allows for emergent electronic access when needed. Many companies believe there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, the risk level to the BES, in terms of reliability, is increased. |
| **Response: Response: -While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br><br>**-In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.**<br><br>**-The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| Salt River Project | Negative | The interpretation does not clearly provide a definition that escorted electronic access is prohibited. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| Dominion | No | The following Dominion responses are provided in order of the questions asked by WECC:1. The interpretation that individuals on the list of personnel authorized for cyber or unescorted physical access to CCAs are subject to CIP-004-1 R2, R3 (with allowed restrictions), and R4 is appropriate.2. CIP-004-1-R4 specifically addresses authorized access and does not state that "all cyber access to Critical Cyber Assets must be authorized". CIP-004-1-R2 and CIP-004-1-R3 (with allowed restrictions) apply to "personnel having authorized cyber or authorized unescorted physical access". The lack of an expression such as "escorted electronic access" does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard.3. The concept of "escorted electronic access" is absent from CIP-004-1. Absent a standard, it should be up to each Registered Entity to determine by internal policy whether or not escorted electronic access should be allowed. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| Pepco Holdings Inc & Affiliates | No | It is understood why the SDT applied a strict interpretation which results in no change to the existing standard. The requested interpretation would have changed the meaning and reach of the standard. However there still remains a very serious real problem. There is a need to allow cyber access to a vendor on some sort of an emergency basis without meeting R2 and R3. The Impact Statement in the Request for Interpretation submitted by WECC is a very serious problem for many entities that could result in a high risk or serious system reliability problem. |
| **Response: The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| FirstEnergy | No | There is an inherent flaw in the interpretation because it is based on an inactive standard CIP-004-1. The current effective standard is CIP-004-3 which differs in a significant way from CIP-004-1. Version 3 of this standard now allows exceptions in emergency situations as stated from the phrase "except in specified circumstances such as an emergency" which is included in R2.1 and R3. This specifically affects the answer to WECC's third question. Remote and on-site cyber access should be allowed under supervision during emergency situations and it would be very difficult to assure that all personnel offering remote assistance in these situations were assessed per the requirements of CIP-004.A second inherent flaw is that the interpretation is based on an inactive standard CIP-006-1. The current effective standard CIP-006-3 expressly describes visitor supervision requirements. Per CIP-006-3, R1.6, visitors are required to be continuously escorted within Physical Security Perimeters. This revised requirement should be integrated into the answers to WECC's second and third question.Therefore, we suggest the team revise the interpretation to only make reference to the current Version 3 standards, and add language in the interpretation that there are exceptions for emergency situations as specified by the entity per CIP-003 which requires details of those emergency situations. |
| **Response: The IDT considered all versions of the CIP standards throughout the Interpretation process as entities could still undergo audit proceedings to CIP Version 1. When an interpretation is requested for an ealier version of a standard, and the issue for which interpretation is requested persists in subsequent versions, the interpretation applies to all of the versions of the standard in which the language being interpreted exists. With regard to the emergency exceptions, the IDT notes that CIP Version 1 allowed for a 30 and 90 day provision with respect to Personnel Risk Assessments and Training. Through the Standards development process this language was removed and replaced with language in CIP Version 2 (which is retained in subsequent approved versions) to allow exceptions to the training and personnel risk assessment authorization requirements in specified** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **circumstances, including emergency situations.** | | |
| ACES Power Marketing Collaborators | No | This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus, maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. Three terms are defined or bounded outside the standards development process. These terms include: authorized access, cyber access and physical access. We will not repeat our arguments regarding this expansion of the standard here. They can be found in question 2. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary to the interpretation, most (probably all) registered entities have a formal |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed.We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert, software expert). |
| **Response: -The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations, which is consistent with FERC Order No. 706, Paragraph 431. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| -The IDT notes that the FERC Order No. 706 issued directives for development of the CIP standards, and the approved standards that resulted from consideration of Order No. 706 are the relevant requirements that are mandatory and enforceable on Responsible Entities under a particular standard. FERC Order No. 706 itself does not create or allow an exception to a reliability standard. Furthermore, the IDT disagrees that Paragraph 431 merely directs that "limited exceptions should be allowed"; rather, Paragraph 431 suggests that the limited exceptions to required training before obtaining access relate to specific conditions, "such as during emergencies, subject to documentation and mitigation." (FERC Order No. 706, Paragraph 431). That is consistent with the IDT's recognition of the provisions for emergency and planned access.<br>-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.<br>-With regard to the emergency exceptions and FERC Order No. 706, the IDT notes that CIP Version 1 allowed for a 30 and 90 day provision with respect to Personnel Risk Assessments and Training. Through the Standards development process this language was removed and replaced with language in CIP Version 2 and beyond to allow exceptions to the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.<br>-In response to the comments submitted in regard to an entity's list, maintenance of a list, management approval processes, and list inconsistencies with actual physical and cyber access controls, the IDT cannot make interpretations on how specific entities are achieving compliance. The IDT understands the concerns raised by the commenter, however the IDT understands that each entity has unique processes for achieving and demonstrating compliance. | | |
| Southern Company | No | Comments: Question 2 and 3 from the Request for Interpretation are not answered by the interpretation. The answers simply describe how the CIP standards do not address the questions being asked. The standards do not address the scenario contemplated by the line of questioning and should be remanded to the CIP SDT to fix in version 5 of the standards.Comment:Vendor support personnel dispatched to the various generation sites are selected base upon their physical availability and the expertise required on the projects. It is a difficult task to provide ongoing training and background checks for every potential individual from numerous vendors supporting a variety of systems. It is near impossible to monitor the ongoing employment status of this large number of vendor personnel, to assure timely removal from the access control list, that will be required if implemented as discussed in the proposed interpretation.At present, vendor personnel supplying |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | setup/support may work freely on pre-shipped non-installed systems. This trusted relationship should be extended, to similar individuals under escort at the equipment site. If the support function requires that changes be made to systems, having site personnel follow the direction of the vendor expert presents an increase potential for error, while adding marginal security benefits. |
| **Response: Thank You for your comment. The IDT must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. Modifications to an approved Standard must be addressed within the Standards development process, the IDT encourages the commenter to submit the comments to the SDT working on CIP V5.** | | |
| City of Garland | No | Disagree with the concept of there being no escorted Cyber Access. If someone with authorized access is working with a vendor or contractor on an issue, the system is more secure than if you give him authorized access just because he has a PRA and has had CIP training. Take for example, Hector Xavier Monsegur, the notorious hacker known as Sabu and leader of LulzSec. Because of his cooperation and work with the FBI and other agencies, he may end up with his record cleansed or at least be able to put on a resume his work with the FBI. Eight years from now, a 7 year criminal background check could be clear. If a company were to utilize him for a short term issue, would the company be more secure with him being "escorted" or with him being issued authorized access and allowed free access. It is noted in your supporting comments that the standard requirements do not state specifically that escorted cyber access is permitted. On the other hand, the standard requirements do not have statements preventing escorted cyber access either. Which is more secure? |
| **Response: -Thank You for your comment. While the effectiveness of personnel risk assessment and Training controls are an interesting theoretical discussion, the IDT must provide an interpretation that meets the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| -While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. | | |
| NextEra Energy Inc. | No | As written, this interpretation should either be dismissed as in appropriate or the answers re-written to be clearer and more responsive. See answers to question 1 and 2. |
| Response: Thank you for your comment. See response to commenter in Question 2. | | |
| Ingleside Cogeneration LP | No | Ingleside Cogeneration LP believes that the interpretation is an overly-literal reading of CIP-004 and may hamper routine technical support processes with no demonstrable reduction in cyber-risk . The power and convenience of remote vendor maintenance may be unavailable to all but the largest utilities should costs rise because of it. Such a result will actually diminish BES reliability as access to highly competent technical support and maintenance personnel becomes restricted.There may be acceptable solutions, however. It would seem that a single cyber certification of vendors such as Cisco and GE could be referenced in thousands of individual security policies. Alternatively, the industry could provide a single generic cyber training package and employee background check method for vendors. We would hope that NERC takes a leadership position in resolving these complex issues.Lastly, the industry needs more direction than that provided in the circular response to the first question. The project team essentially states that the Responsible Entity must determine who has authorized access to their Critical Cyber Assets and include them on an access list. That list will then define authorized access - leaving the door open for a wide variety of resolutions. |
| Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **-The IDT understands this concern, but notes that the greater standards development process is better equipped to review such a concept, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."<br>-The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed.** | | |
| MidAmerican Energy Company | No | The request is asking how to comply with one or more requirements in a specific situation with vendor support. Requests as to how to comply, per the Rules of Procedure, do not meet the valid criteria of an interpretation request. While we agree with the conclusion in the proposed response, the draft response restates information that already is in the standard. |
| **Response: The WECC RFI is seeking interpretation of a requirement, and the IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. While the IDT agrees that the interpretation has compliance application implications, on balance, the IDT and most commenters agree that the interpretation is validly asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.** | | |
| Ameren | No | The CIP-004 R4 IDT interpretation relies on incorrect logic in stating that Standard does not allow for escorted (supervised) cyber access to cyber assets solely because "unescorted cyber" is not explicitly included in the CIP-004 R4 "list". We agree with the idea put forth in the Requirement that anyone with unfettered cyber access is a potential danger and in like manner, so would anyone with unescorted physical access. However, the reason the Requirement does not require those with escorted cyber access to be listed is not because such access is somehow not contemplated or not permitted but rather because, like escorted physical access, these individuals, and their actions, are well monitored and controlled and do not need the extra care and handling that ensues from being on "The List" for those free to take independent action. The mere fact that they do not need further "handling" does not mean in any way that they do not exist or that this in not permitted. We are concerned that IDT is |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | using a classic argument from the negative to imply something is impermissible on that such use is not contemplated merely because it is absent from a list of threat types that need to be addressed. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT also notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** | | |
| United Illuminating Company | No | The Interpretation DT correctly states that CIP-004 R2 and R3 apply to individuals on a list designating them with authorized cyber access or authorized unescorted physical access to Critical Cyber Assets. The Interpretation DT makes an error in stating that CIP-004 limits the type of cyber access to a Critical Cyber Assets to only authorized individuals, that is, there is no opportunity to implement supervised remote access via terminal session (i.e. Webex) to support personnel not on the authorized cyber access list.The Reliability standards do not provide a definitive statement of the types of access allowed to Critical Cyber Assets. The Standards only provide the program requirements for three types of access; authorized physical, escorted physical, and authorized cyber. By not providing a definitive list of the types of access the original Drafting team did not exclude the type of access under review in this interpretation, that is, supervised cyber access via terminal session.At the time the Reliability standards was approved the concept of supervised remote access was known. The Interpretation Drafting Team can only conclude that the original Standard Drafting Team did not list specific requirements for this type of access. The Interpretation Drafting Team cannot conclude that this type of access was prohibited. The fact that CIP-007 does not contain a specific unescorted cyber access provision is irrelevant. CIP-007 R5 requires technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Supervised access via Webex is not unauthorized system access. When terminal session access is utilized, the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | activity is tracked by the Company. R5 does not state all authorized user activity, the Interpretation drafting team is adding the word authorized in its response and is expanding the scope.This conclusion is more sensible for service vendors and SCADA system providers. The Interpretation Drafting Team's interpretation would require, as the requestor noted, large vendors (such as CISCO) to take every entities cyber training course and submit to multiple background checks. This would be compliance for compliance sake and not for security. The Interpretation should have stated that the names of authorized individuals are maintained on a list. These individuals are required to comply with CIP-004 R2 through R4. Supervisory Cyber Access via terminal session is not prohibited explicitly by the Standards and is therefore allowed. There are no additional Reliability requirements for such access beyond those described in Standards CIP-002 through CIP-009. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. -Considering the Standards Development Process is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** | | |
| Progress Energy | No | Progress Energy disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or onsite cyber access). Registered Entities should be able to allow vendors providing support temporary, indirect, and monitored access to in scope NERC CIP assets via remote terminal sessions (Live Mtg, Webex, etc) (just as escorted physical access is allowed) without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. In addition, Registered Entities should be able to allow vendors providing onsite temporary support escorted cyber access without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4.There are multiple NERC CIP support vendors that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard. This |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | includes process control vendors not just IT vendors. Honeywell, GE, ABB, Siemens, Babcock and Wilcox, Emerson, GTE, Wood Group are all DCS vendors/tuners that may need to provide escorted cyber access at Progress Energy and throughout the industry. Not allowing for escorted cyber access could have adverse impacts to BES Reliability since some of this work is needed not only during emergencies but also for ongoing maintenance. Long term service agreements are in place with these vendors that have warranty implications that require escorted cyber support for various process control systems. Many Registered Entities rely on these vendors/tuners to provide their expertise in support of continual operations for proprietary systems and do not employ resources with these specialized skill sets. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br>**-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Waterfall Security Solutions | No? | Unidirectional remote screen view products using hardware-enforced unidirectional communications or "data diodes" can securely show remote, unauthorized personnel the contents of screens on Critical Cyber Assets which are inside of an ESP. The technology allows remote personnel to watch and advise as authorized individuals carry out cyber access to those CCAs without introducing any risk that the remote personnel can directly influence the monitored CCAs in any way. This mechanism addresses WECC's concern regarding being "excessively burdened by limiting access to timely support." Since unidirectional remote screen view technology prevents the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | unauthorized observer from carrying out any direct cyber access, the unidirectional technology should have been identified in the interpretation as a legitimate form of supervised remote access. |
| **Response: Without commenting on specific technology, this comment raises access control and information protection considerations that are both outside the scope of this interpretation.** | | |
| Salt River Project | No | As written we disagree with the IDT team's interpretation of CIP-004. We recognize CIP-004 does not include the concept of any words relating to "escorting" or "supervision" in the requirement language. However, the interpretation is not clearly defined and reaches the conclusion that escorted electronic access is prohibited because a formal electronic access escorting requirement is not defined. It appears this conclusion was based on the fact that CIP-006 clearly defines "escorted" or "supervised" physical access to cyber assets. We believe this type of assumption sets a bad precedent for future interpretations.Additionally we believe this interpretation won't allow emergent electronic access when needed. We believe there is little or no risk associated with allowing escorted access to a known contracted support vendor, when support is needed. In fact we believe prohibiting this type of access increases the risk level to the BES. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Austin Energy | No | We believe NERC should acknowledge that "escorted" cyber access is legitimate. If one of our employees is monitoring the cyber activities of the escorted vendor, our |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | employee could terminate the session if the vendor began to take inappropriate actions. This is akin to the situation for escorted physical access. As long as the person is escorted, if s/he begins to take inappropriate action, the escort can take appropriate responsive action. |
| **Response: As written the Standards do not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Essential Power, LLC | No | In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation.In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support.Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard.There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access. |
| **Response: The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Midwest ISO | No | MISO respectfully submits that the IDT's proposed Interpretation of the phrase "authorized access" is unsupported by the plain language of CIP-004. The phrase "authorized access," which is the subject of the Interpretation, does not appear in CIP-004. Instead, the Standard uses the phrase "authorized cyber or authorized unescorted physical access." MISO understands that the question posed by the requestor utilized the term "Authorized Access", but respectfully submits that the IDT should have provided clarification specifically regarding authorized cyber access and authorized unescorted cyber access, which clarification would have resulted in entities ability to more directly apply the interpretation to its compliance efforts under CIP-004-1, R2. Moreover, the IDT's explanation of "authorized access" merely refers back to the requirements associated with access without providing the requested clarification. As a result, MISO does not agree with the Interpretation as to the answer provided in response to Question 1. As to the proposed answers to Questions 2 and 3, MISO respectfully submits that, without the specific clarification requested under Question 1, the Interpretation's conclusions are not sufficiently supported by the text of CIP-004. |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.** | | |
| CRSI | No | The response to question 1 attempts to define authorized access. The definition, even if local to CIP-004, should be expanded to include an indication that authorized access indicates personnel with approval to access Critical Cyber Assets. The presence of a person's name on a maintained list could be in error and would not be an indication of authorized access. |
| **Response: The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized.** | | |
| MISO Standards Collaborators | | We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access. |
| **Response: The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard.** | | |
| Omaha Public Power District | | From NERC Comment form (Sorry we did not get it submitted on time) 1. The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | application of a requirement? 0 The request is asking for clarity on the meaning of a requirement. 1 The request is asking for clarity on the application of a requirement. Comments: N/A 2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard? 1 The interpretation expands the reach of the standard. 0 The interpretation does not expand the reach of the standard. Comments: OPPD respectfully disagrees with the proposed interpretation provided by NERC in response to questions submitted by WECC. Utilizing standards that are not in direct relation to the question being proposed contains no true definition or answer. This type of response sets an unacceptable precedence of using different standards and requirements to justify an interpretation. 3. Do you agree with this interpretation? If not, please explain specifically what you disagree with. 0 Yes 1 No Comments: In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, OPPD does not believe the interpretation allows for emergent electronic access when needed. OPPD believes there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, OPPD feels the risk level to the BES, in terms of reliability, is indeed increased. |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: -In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.<br>-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.<br>-The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.<br>-Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| Bonneville Power Administration | Yes | |
| Kansas City Power & Light | Yes | |
| ISO/RTO Standards Review Committee | Yes | |
| Imperial Irrigation District (IID) | Yes | |
| PacifiCorp | Yes | |
| Xcel Energy | Yes | |
| NIPSCO | Yes | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| American Transmission Company, LLC | Yes | |
| Minnesota Power | Yes | |
| Duke Energy | Yes | |
| Independent Electricity System Operator | Yes | |
| E.ON CLIMATE & RENEWABLES | Yes | |
| Northeast Power Coordinating Council | Yes | |
| Great River Energy | Negative | Please see the formal comments submitted by ACES Power Marketing. |
| Brazos Electric Power Cooperative, Inc. | Negative | Please see comments to be submitted by ACES Power Marketing. |
| FirstEnergy Solutions | Negative | Please see FirstEnergy's comments submitted through the formal comment period. |
| Occidental Chemical | Negative | See comments submitted from Ingelside Cogeneration LP |
| Omaha Public Power District | Negative | Please Doug Peterchuck's comments. |
| **Response: Thank you for your comments.** | | |

END OF REPORT

**Exhibit D**

Complete Record of Development of the interpretation of Requirements R2, R3, and R4 of CIP-004-4 — Personnel and Training.

**Project 2009-26**
**Interpretation of CIP-004-1**

Related Files

**Status:**
Adopted by the Board of Trustees on May 24, 2012, pending regulatory approval.

**Purpose / Industry Need:**
WECC requested an interpretation of CIP-004-1 Requirements R2 through R4.

| Draft | Action | Dates | Results | Consideration of Comments |
|---|---|---|---|---|
| Interpretation of CIP-004-x, Requirements R2-R4<br>Clean**(18)**<br><br>**Supporting Documents**<br>CIP-004-3**(19)** | Recirculation Ballot<br><br>Info**(20)**<br><br>Vote>> | 4/20/12 - 4/30/12 | Summary **(21)**<br><br>Full Record**(22)** | |
| **Draft 2**<br><br>Interpretation of CIP-004-x, Requirements R2-R4<br>Clean**(8)** \| Redline to last posted**(9)**<br><br>**Supporting Documents**<br>CIP-004-3**(10)**<br>Unofficial Comment Form (Word)**(11)** | Successive Ballot<br><br>Updated Info**(12)**<br>Vote>><br><br>Info**(13)** | 03/13/12 - 03/23/12 (closed) | Summary **(14)**<br><br>Full Record**(15)** | |
| | Formal Comment Period<br><br>Submit Comments >> | 02/07/12 - 03/23/12 (closed) | Comments Received **(16)** | Consideration of Comments **(17)** |
| | Ballot Pool<br><br>Join>> | 02/07/12 - 03/08/12 | | |

| | | | | |
|---|---|---|---|---|
| | | (closed) | | |
| | | | | |
| WECC<br>CIP-004-1 Requirements R2-R4<br><br>Request for Interpretation **(1)**<br><br>Interpretation **(2)** | Initial Ballot<br><br>Vote>> \| Info **(3)** | 01/06/10 - 01/19/10 (closed) | Summary **(5)**<br><br>Final Results **(6)** | Consideration of Comments **(7)** |
| | Pre-ballot Review<br><br>Join>> \| Info **(4)** | 12/07/09 - 01/06/10 (closed) | | |
| To download a file click on the file using your right mouse button, then save it to your computer in a directory of your choice. | | | | |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Note: an Interpretation cannot be used to change a standard.**

| Request for an Interpretation of a Reliability Standard | |
|---|---|
| Date submitted: 10/15/09 | |
| Date accepted: 10/23/09 | |
| **Contact information for person requesting the interpretation:** | |
| Name: | John Van Boxtel |
| Organization: | Western Electricity Coordinating Council |
| Telephone: | 360-713-9090 |
| E-mail: | jvanboxtel@wecc.biz |
| **Identify the standard that needs clarification:** | |
| Standard Number: | CIP-004-1 |
| Standard Title: | Cyber Security – Personnel and Training |
| **Identify specifically what requirement needs clarification:** | |

Requirement Number and Text of Requirement: R2, R3, and R4

***R2.*** *Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for* ***personnel having authorized cyber or authorized unescorted physical access*** *to Critical Cyber Assets, and review the program annually and update as 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.*

***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****. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access.*

***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.*

**Clarification needed (emphasis added):**
Specifically, the WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

**Background**
Through previously published documents, both NERC and FERC have indicated that the intent of the CIP-004 Standard was to document training, risk assessment, and access to Critical Cyber Assets in situations where personnel have direct and unmonitored access to critical cyber assets, as opposed to and distinguishable from **supervised access.**

The question asked in Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training is: "*What is meant by 'authorized cyber access?'" The answer provided is:*

> *The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.* (emphasis added)

This answer is also consistent with a similar description of escorted access provided in FERC Order 706, page 116, paragraph 432, in which the Commission stated:

> *Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power system. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.* (emphasis added)

**Identify the material impact associated with this interpretation:**

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

**Material Impact**
If "Authorized Access" includes temporary support access provided in a supervised manner, then there is a potential for many Registered Entities to either be noncompliant while seeking support, or excessively burdened by limiting access to timely support. This situation is particularly likely from large non-utility vendors (such as Cisco Systems) that are either unable or unwilling to provide dedicated support personnel who have complied with each

individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard.

Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations:

- Training covering the specific policies, access controls, and procedures as developed by each individual Registered Entity.
- A personnel risk assessment for all support personnel provided by each individual vendor, based on the cyber security training program developed by each individual Registered Entity.
- Timely updates to each Registered Entity's access list of all support personnel provided by each individual vendor, including changes in personnel at the vendor within the timeframes prescribed by the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Note: an Interpretation cannot be used to change a standard.**

| Request for an Interpretation of a Reliability Standard |
|---|
| Date submitted: 10/15/09 |
| Date accepted: 10/23/09 |
| **Contact information for person requesting the interpretation:** |
| Name: John Van Boxtel |
| Organization: Western Electricity Coordinating Council |
| Telephone: 360-713-9090 |
| E-mail: jvanboxtel@wecc.biz |
| **Identify the standard that needs clarification:** |
| Standard Number: CIP-004-1 |
| Standard Title: Cyber Security – Personnel and Training |
| **Identify specifically what requirement needs clarification:** |

**Requirement Number and Text of Requirement:** R2, R3, and R4

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

**Clarification needed (emphasis added):**

Specifically, the WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would

temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

**Background**

Through previously published documents, both NERC and FERC have indicated that the intent of the CIP-004 Standard was to document training, risk assessment, and access to Critical Cyber Assets in situations where personnel have direct and unmonitored access to critical cyber assets, as opposed to and distinguishable from **supervised access.**

The question asked in Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training is: "*What is meant by 'authorized cyber access?'" The answer provided is:*

> *The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.* (emphasis added)

This answer is also consistent with a similar description of escorted access provided in FERC Order 706, page 116, paragraph 432, in which the Commission stated:

> *Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power system. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.* (emphasis added)

**Identify the material impact associated with this interpretation:**

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

**Material Impact**

If "Authorized Access" includes temporary support access provided in a supervised manner, then there is a potential for many Registered Entities to either be noncompliant while seeking support, or excessively burdened by limiting access to timely support. This situation is particularly likely from large non-utility vendors (such as Cisco Systems) that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard.

Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations:

- Training covering the specific policies, access controls, and procedures as developed by each individual Registered Entity.
- A personnel risk assessment for all support personnel provided by each individual vendor, based on the cyber security training program developed by each individual Registered Entity.
- Timely updates to each Registered Entity's access list of all support personnel provided by each individual vendor, including changes in personnel at the vendor within the timeframes prescribed by the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

## Project 2009-26: Response to Request for an Interpretation of NERC Standard CIP-004-1 for the Western Electricity Coordinating Council

The following interpretation of NERC Standard CIP-004-1 Cyber Security — Personnel & Training, Requirements R2, R3, and R4, was developed by the Cyber Security Order 706 SAR drafting team.

### Requirement Number and Text of Requirement

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

### Question

The WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

### Response

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Initial Ballot Window Open

## January 6–19, 2010

**Now available at: https://standards.nerc.net/CurrentBallots.aspx**

### Project 2009-26: Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (WECC)

An initial ballot window for an interpretation of standard CIP-004-1 — Cyber Security — Personnel & Training, Requirements R2, R3, and R4, for WECC is now open **until 8 p.m. EST on January 19, 2010**.

### Instructions

Members of the ballot pool associated with this project may log in and submit their votes from the following page: https://standards.nerc.net/CurrentBallots.aspx

### Next Steps

Voting results will be posted and announced after the ballot window closes.

### Project Background

WECC requested clarification regarding temporary access by vendors. WECC asked for clarification on 1) the definition of "authorized access," 2) whether or not specific requirements in CIP-004-1 apply to supervised vendors, and 3) the appropriate level of supervision. If approved, this interpretation would apply to CIP-004-1, CIP-004-2, and CIP-004-3.

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

### Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

*For more information or assistance,*
*please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Ballot Pool and Pre-ballot Window
## December 7, 2009–January 6, 2010

**Now available at: https://standards.nerc.net/BallotPool.aspx**

### Project 2009-26: Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (WECC)

An interpretation of standard CIP-004-1 — Cyber Security — Personnel & Training, Requirements R2, R3, and R4, for WECC is posted for a 30-day pre-ballot review. Registered Ballot Body members may join the ballot pool to be eligible to vote on this interpretation **until 8 a.m. EST on January 6, 2010**.

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list server for this ballot pool is: bp-2009-26_RFI_WECC_CIP_in.

### Next Steps

Voting will begin shortly after the pre-ballot review closes.

### Project Background

WECC requested clarification regarding temporary access by vendors. WECC asked for clarification on 1) the definition of "authorized access," 2) whether or not specific requirements in CIP-004-1 apply to supervised vendors, and 3) the appropriate level of supervision.

If approved, this interpretation would apply to CIP-004-1, CIP-004-2, and CIP-004-3.

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

### Standards Development Process

The Reliability Standards Development Procedure contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

*For more information or assistance,*
*please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Initial Ballot Results

**Now available at: https://standards.nerc.net/Ballots.aspx**

**Project 2009-26: Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (WECC)**
The initial ballot for an interpretation of standard CIP-004-1 — Cyber Security — Personnel & Training, Requirements R2, R3, and R4, for WECC ended on January 19, 2010.

**Ballot Results**
Voting statistics are listed below, and the Ballot Results Web page provides a link to the detailed results:

Quorum: 84.21%
Approval: 42.24%

Since at least one negative ballot included a comment, these results are not final. A second (or recirculation) ballot must be conducted. Ballot criteria are listed at the end of the announcement.

### Next Steps
As part of the recirculation ballot process, the drafting team must draft and post responses to voter comments. The drafting team will also determine whether or not to make revisions to the balloted item(s). Should the team decide to make revisions, the revised item(s) will return to the initial ballot phase.

### Project Background
WECC requested clarification regarding temporary access by vendors. WECC asked for clarification on 1) the definition of "authorized access," 2) whether or not specific requirements in CIP-004-1 apply to supervised vendors, and 3) the appropriate level of supervision. If approved, this interpretation would apply to CIP-004-1, CIP-004-2, and CIP-004-3.

The request and interpretation are posted on the project page:
http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

### Standards Development Process
The *Reliability Standards Development Procedure* contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate.

### Ballot Criteria
Approval requires both a (1) quorum, which is established by at least 75% of the members of the ballot pool for submitting either an affirmative vote, a negative vote, or an abstention, and (2) A two-thirds majority of the weighted segment votes cast must be affirmative; the number of votes cast is the sum of affirmative and negative votes, excluding abstentions and nonresponses. If there are no negative votes with reasons from the first ballot, the results of the first ballot shall stand. If, however, one or more members submit negative votes with reasons, a second ballot shall be conducted.

*For more information or assistance,*
*please contact Shaun Streeter at shaun.streeter@nerc.net or at 609.452.8060.*

## Ballot Results

| | |
|---|---|
| **Ballot Name:** | Project 2009-26 - Interpretation - WECC - CIP-004-1_in |
| **Ballot Period:** | 1/6/2010 - 1/19/2010 |
| **Ballot Type:** | Initial |
| **Total # Votes:** | 208 |
| **Total Ballot Pool:** | 247 |
| **Quorum:** | **84.21 % The Quorum has been reached** |
| **Weighted Segment Vote:** | 42.24 % |
| **Ballot Results:** | **The standard will proceed to recirculation ballot.** |

## Summary of Ballot Results

| Segment | Ballot Pool | Segment Weight | Affirmative # Votes | Affirmative Fraction | Negative # Votes | Negative Fraction | Abstain # Votes | No Vote |
|---|---|---|---|---|---|---|---|---|
| 1 - Segment 1. | 67 | 1 | 22 | 0.415 | 31 | 0.585 | 6 | 8 |
| 2 - Segment 2. | 12 | 1 | 2 | 0.2 | 8 | 0.8 | 1 | 1 |
| 3 - Segment 3. | 59 | 1 | 18 | 0.419 | 25 | 0.581 | 8 | 8 |
| 4 - Segment 4. | 16 | 1 | 4 | 0.308 | 9 | 0.692 | 2 | 1 |
| 5 - Segment 5. | 46 | 1 | 15 | 0.455 | 18 | 0.545 | 2 | 11 |
| 6 - Segment 6. | 26 | 1 | 8 | 0.471 | 9 | 0.529 | 4 | 5 |
| 7 - Segment 7. | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 - Segment 8. | 7 | 0.5 | 4 | 0.4 | 1 | 0.1 | 0 | 2 |
| 9 - Segment 9. | 6 | 0.4 | 1 | 0.1 | 3 | 0.3 | 1 | 1 |
| 10 - Segment 10. | 8 | 0.6 | 4 | 0.4 | 2 | 0.2 | 0 | 2 |
| **Totals** | **247** | **7.5** | **78** | **3.168** | **106** | **4.332** | **24** | **39** |

## Individual Ballot Pool Results

| Segment | Organization | Member | Ballot | Comments |
|---|---|---|---|---|
| 1 | Allegheny Power | Rodney Phillips | | |
| 1 | AltaLink Management Ltd. | Rick Spyker | Negative | View |
| 1 | Ameren Services | Kirit S. Shah | Negative | View |
| 1 | American Electric Power | Paul B. Johnson | Affirmative | |
| 1 | American Transmission Company, LLC | Jason Shaver | Negative | View |
| 1 | Avista Corp. | Scott Kinney | Negative | |
| 1 | Baltimore Gas & Electric Company | John J. Moraski | Affirmative | |
| 1 | BC Transmission Corporation | Gordon Rawlings | Affirmative | |

| | | | | |
|---|---|---|---|---|
| 1 | Black Hills Corp | Eric Egge | | |
| 1 | Bonneville Power Administration | Donald S. Watkins | Negative | View |
| 1 | Brazos Electric Power Cooperative, Inc. | Tony Kroskey | Negative | View |
| 1 | CenterPoint Energy | Paul Rocha | Negative | View |
| 1 | Central Maine Power Company | Brian Conroy | Negative | |
| 1 | City of Vero Beach | Randall McCamish | Negative | |
| 1 | Cleco Power LLC | Danny McDaniel | Abstain | |
| 1 | Consolidated Edison Co. of New York | Christopher L de Graffenried | Affirmative | |
| 1 | Dominion Virginia Power | William L. Thompson | Negative | |
| 1 | Duke Energy Carolina | Douglas E. Hils | Affirmative | |
| 1 | East Kentucky Power Coop. | George S. Carruba | | |
| 1 | Entergy Corporation | George R. Bartlett | Negative | |
| 1 | Exelon Energy | John J. Blazekovich | Affirmative | |
| 1 | FirstEnergy Energy Delivery | Robert Martinko | Negative | View |
| 1 | Florida Keys Electric Cooperative Assoc. | Dennis Minton | Negative | |
| 1 | Gainesville Regional Utilities | Luther E. Fair | Abstain | |
| 1 | Georgia Transmission Corporation | Harold Taylor, II | Negative | View |
| 1 | Hoosier Energy Rural Electric Cooperative, Inc. | Robert Solomon | | |
| 1 | Hydro One Networks, Inc. | Ajay Garg | Abstain | |
| 1 | Hydro-Quebec TransEnergie | Albert Poire | Affirmative | |
| 1 | Idaho Power Company | Ronald D. Schellberg | Negative | View |
| 1 | ITC Transmission | Elizabeth Howell | Negative | |
| 1 | Lakeland Electric | Larry E Watt | Negative | View |
| 1 | Lee County Electric Cooperative | John W Delucca | Abstain | |
| 1 | Lincoln Electric System | Doug Bantam | Affirmative | |
| 1 | Long Island Power Authority | Jonathan Appelbaum | Affirmative | |
| 1 | Lower Colorado River Authority | Martyn Turner | Negative | |
| 1 | MEAG Power | Danny Dees | Affirmative | |
| 1 | MidAmerican Energy Co. | Terry Harbour | Negative | View |
| 1 | Northeast Utilities | David H. Boguslawski | Abstain | |
| 1 | Northern Indiana Public Service Co. | Kevin M Largura | Affirmative | |
| 1 | NorthWestern Energy | John Canavan | Negative | View |
| 1 | Oklahoma Gas and Electric Co. | Marvin E VanBebber | Affirmative | |
| 1 | Omaha Public Power District | Lorees Tadros | | |
| 1 | Orlando Utilities Commission | Brad Chase | Affirmative | |
| 1 | Otter Tail Power Company | Lawrence R. Larson | Affirmative | |
| 1 | Pacific Gas and Electric Company | Chifong L. Thomas | | |
| 1 | PacifiCorp | Mark Sampson | Negative | |
| 1 | Platte River Power Authority | John C. Collins | | |
| 1 | Potomac Electric Power Co. | Richard J. Kafka | Affirmative | View |
| 1 | PowerSouth Energy Cooperative | Larry D. Avery | Negative | |
| 1 | PP&L, Inc. | Ray Mammarella | Affirmative | |
| 1 | Progress Energy Carolinas | Sammy Roberts | Affirmative | |
| 1 | Public Service Electric and Gas Co. | Kenneth D. Brown | Affirmative | View |
| 1 | Sacramento Municipal Utility District | Tim Kelley | Negative | View |
| 1 | Salt River Project | Robert Kondziolka | Negative | View |
| 1 | SCE&G | Henry Delk, Jr. | Affirmative | |
| 1 | Seattle City Light | Pawel Krupa | Negative | View |
| 1 | Sierra Pacific Power Co. | Richard Salgo | Negative | View |
| 1 | Southern California Edison Co. | Dana Cabbell | Negative | View |
| 1 | Southern Company Services, Inc. | Horace Stephen Williamson | Negative | View |
| 1 | Southern Illinois Power Coop. | William G. Hutchison | Negative | |
| 1 | Southwest Transmission Cooperative, Inc. | James L. Jones | Abstain | |
| 1 | Southwestern Power Administration | Gary W Cox | Affirmative | |
| 1 | Tri-State G & T Association Inc. | Keith V. Carman | Negative | View |
| 1 | Tucson Electric Power Co. | John Tolo | Negative | View |
| 1 | Westar Energy | Allen Klassen | Affirmative | |
| 1 | Western Area Power Administration | Brandy A Dunn | Affirmative | |
| 1 | Xcel Energy, Inc. | Gregory L Pieper | | |
| 2 | Alberta Electric System Operator | Jason L. Murray | Abstain | |
| 2 | BC Transmission Corporation | Faramarz Amjadi | Affirmative | |
| 2 | California ISO | Greg Tillitson | Negative | |
| 2 | Electric Reliability Council of Texas, Inc. | Chuck B Manning | Negative | View |
| 2 | Florida Municipal Power Pool | Thomas E Washburn | Affirmative | |
| 2 | Independent Electricity System Operator | Kim Warren | Negative | View |
| 2 | ISO New England, Inc. | Kathleen Goodman | Negative | View |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 2 | Midwest ISO, Inc. | Jason L Marshall | Negative | View |
| 2 | New Brunswick System Operator | Alden Briggs | Negative | View |
| 2 | New York Independent System Operator | Gregory Campoli | Negative | View |
| 2 | Salt River Project | Jeffrey L. Packer | | |
| 2 | Southwest Power Pool | Charles H Yeung | Negative | |
| 3 | Alabama Power Company | Bobby Kerley | Negative | View |
| 3 | Allegheny Power | Bob Reeping | | |
| 3 | American Electric Power | Raj Rana | Affirmative | |
| 3 | Arizona Public Service Co. | Thomas R. Glock | Negative | View |
| 3 | Atlantic City Electric Company | James V. Petrella | Affirmative | |
| 3 | BC Hydro and Power Authority | Pat G. Harrington | Abstain | |
| 3 | Bonneville Power Administration | Rebecca Berdahl | Negative | View |
| 3 | City of Farmington | Linda R. Jacobson | Negative | View |
| 3 | City Public Service of San Antonio | Edwin Les Barrow | Abstain | |
| 3 | Clay Electric Cooperative | Howard M. Mott Jr. | Abstain | |
| 3 | Cleco Utility Group | Bryan Y Harper | Abstain | |
| 3 | Commonwealth Edison Co. | Stephen Lesniak | Affirmative | |
| 3 | Consolidated Edison Co. of New York | Peter T Yost | Affirmative | |
| 3 | Consumers Energy | David A. Lapinski | Negative | |
| 3 | Cowlitz County PUD | Russell A Noble | Negative | View |
| 3 | Delmarva Power & Light Co. | Michael R. Mayer | Affirmative | |
| 3 | Detroit Edison Company | Kent Kujala | Affirmative | |
| 3 | Dominion Resources, Inc. | Jalal (John) Babik | Negative | View |
| 3 | Duke Energy Carolina | Henry Ernst-Jr | Affirmative | |
| 3 | Entergy Services, Inc. | Matt Wolf | Affirmative | |
| 3 | FirstEnergy Solutions | Joanne Kathleen Borrell | Negative | View |
| 3 | Florida Municipal Power Agency | Joe McKinney | Negative | |
| 3 | Florida Power Corporation | Lee Schuster | Affirmative | |
| 3 | Georgia Power Company | Leslie Sibert | Negative | View |
| 3 | Georgia System Operations Corporation | R Scott S. Barfield-McGinnis | Negative | View |
| 3 | Grays Harbor PUD | Wesley W Gray | Affirmative | |
| 3 | Gulf Power Company | Gwen S Frazier | Negative | View |
| 3 | Hydro One Networks, Inc. | Michael D. Penstone | Abstain | |
| 3 | JEA | Garry Baker | | |
| 3 | Kansas City Power & Light Co. | Charles Locke | | |
| 3 | Kissimmee Utility Authority | Gregory David Woessner | | |
| 3 | Lakeland Electric | Mace Hunter | Affirmative | |
| 3 | Lincoln Electric System | Bruce Merrill | Affirmative | |
| 3 | Louisville Gas and Electric Co. | Charles A. Freibert | Abstain | |
| 3 | MidAmerican Energy Co. | Thomas C. Mielnik | | |
| 3 | Mississippi Power | Don Horsley | Negative | View |
| 3 | Modesto Irrigation District | Jack W Savage | | |
| 3 | Municipal Electric Authority of Georgia | Steven M. Jackson | Abstain | |
| 3 | New York Power Authority | Marilyn Brown | Negative | |
| 3 | Niagara Mohawk (National Grid Company) | Michael Schiavone | Affirmative | |
| 3 | Northern Indiana Public Service Co. | William SeDoris | Affirmative | |
| 3 | Orlando Utilities Commission | Ballard Keith Mutters | Affirmative | |
| 3 | PacifiCorp | John Apperson | Negative | |
| 3 | Platte River Power Authority | Terry L Baker | Negative | View |
| 3 | Progress Energy Carolinas | Sam Waters | Affirmative | |
| 3 | Public Service Electric and Gas Co. | Jeffrey Mueller | Affirmative | View |
| 3 | Public Utility District No. 1 of Chelan County | Kenneth R. Johnson | Negative | View |
| 3 | Public Utility District No. 2 of Grant County | Greg Lange | Negative | View |
| 3 | Sacramento Municipal Utility District | James Leigh-Kendall | Negative | View |
| 3 | Salt River Project | John T. Underhill | Negative | View |
| 3 | San Diego Gas & Electric | Scott Peterson | | |
| 3 | Seattle City Light | Dana Wheelock | Negative | View |
| 3 | South Carolina Electric & Gas Co. | Hubert C. Young | Affirmative | |
| 3 | Southern California Edison Co. | David Schiada | | |
| 3 | Tampa Electric Co. | Ronald L Donahey | Negative | View |
| 3 | Tri-State G & T Association Inc. | Janelle Marriott | Negative | |
| 3 | Wisconsin Electric Power Marketing | James R. Keller | Negative | View |
| 3 | Wisconsin Public Service Corp. | Gregory J Le Grave | Negative | View |
| 3 | Xcel Energy, Inc. | Michael Ibold | Abstain | |
| 4 | Alliant Energy Corp. Services, Inc. | Kenneth Goldsmith | Affirmative | |
| 4 | City of New Smyrna Beach Utilities Commission | Timothy Beyrle | Negative | |

| | | | | |
|---|---|---|---|---|
| 4 | Consumers Energy | David Frank Ronk | Negative | View |
| 4 | Detroit Edison Company | Daniel Herring | Affirmative | |
| 4 | Florida Municipal Power Agency | Frank Gaffney | Negative | |
| 4 | Georgia System Operations Corporation | Guy Andrews | Negative | View |
| 4 | Integrys Energy Group, Inc. | Christopher Plante | Abstain | |
| 4 | Madison Gas and Electric Co. | Joseph G. DePoorter | Affirmative | |
| 4 | Northern California Power Agency | Fred E. Young | | |
| 4 | Ohio Edison Company | Douglas Hohlbaugh | Negative | View |
| 4 | Old Dominion Electric Coop. | Mark Ringhausen | Abstain | |
| 4 | Public Utility District No. 1 of Snohomish County | John D. Martinsen | Negative | View |
| 4 | Sacramento Municipal Utility District | Mike Ramirez | Negative | View |
| 4 | Seattle City Light | Hao Li | Negative | View |
| 4 | Seminole Electric Cooperative, Inc. | Steven R Wallace | Affirmative | |
| 4 | Wisconsin Energy Corp. | Anthony Jankowski | Negative | View |
| 5 | AEP Service Corp. | Brock Ondayko | Affirmative | |
| 5 | Amerenue | Sam Dwyer | Negative | |
| 5 | Avista Corp. | Edward F. Groce | Abstain | |
| 5 | Black Hills Corp | George Tatar | Negative | |
| 5 | Bonneville Power Administration | Francis J. Halpin | Negative | View |
| 5 | City of Tallahassee | Alan Gale | Negative | View |
| 5 | Colmac Clarion/Piney Creek LP | Harvie D. Beavers | Affirmative | |
| 5 | Consolidated Edison Co. of New York | Edwin E Thompson | Affirmative | |
| 5 | Consumers Energy | James B Lewis | Negative | View |
| 5 | Dairyland Power Coop. | Warren Schaefer | | |
| 5 | Detroit Edison Company | Ronald W. Bauer | Affirmative | |
| 5 | Dominion Resources, Inc. | Mike Garton | Negative | View |
| 5 | Entergy Corporation | Stanley M Jaskot | Negative | |
| 5 | Exelon Nuclear | Michael Korchynsky | Affirmative | |
| 5 | FirstEnergy Solutions | Kenneth Dresner | Negative | View |
| 5 | FPL Energy | Benjamin Church | | |
| 5 | Kissimmee Utility Authority | Mike Blough | | |
| 5 | Lakeland Electric | Thomas J Trickey | Negative | |
| 5 | Liberty Electric Power LLC | Daniel Duff | | |
| 5 | Lincoln Electric System | Dennis Florom | Affirmative | |
| 5 | Louisville Gas and Electric Co. | Charlie Martin | Abstain | |
| 5 | New York Power Authority | Gerald Mannarino | | |
| 5 | Northern Indiana Public Service Co. | Michael K Wilkerson | Affirmative | |
| 5 | Northern States Power Co. | Liam Noailles | | |
| 5 | Oklahoma Gas and Electric Co. | Kim Morphis | | |
| 5 | Orlando Utilities Commission | Richard Kinas | Affirmative | |
| 5 | Pacific Gas and Electric Company | Richard J. Padilla | Affirmative | |
| 5 | PacifiCorp | Sandra L. Shaffer | Negative | |
| 5 | Portland General Electric Co. | Gary L Tingley | Negative | View |
| 5 | PPL Generation LLC | Mark A. Heimbach | Affirmative | |
| 5 | Progress Energy Carolinas | Wayne Lewis | Affirmative | |
| 5 | PSEG Power LLC | David Murray | Affirmative | View |
| 5 | RRI Energy | Thomas J. Bradish | Negative | View |
| 5 | Sacramento Municipal Utility District | Bethany Wright | Negative | View |
| 5 | Salt River Project | Glen Reeves | Negative | View |
| 5 | Seattle City Light | Michael J. Haynes | Negative | View |
| 5 | Seminole Electric Cooperative, Inc. | Brenda K. Atkins | | |
| 5 | South California Edison Company | Ahmad Sanati | | |
| 5 | South Carolina Electric & Gas Co. | Richard Jones | Affirmative | |
| 5 | Southern Company Generation | William D Shultz | Negative | |
| 5 | Tenaska, Inc. | Scott M. Helyer | Affirmative | |
| 5 | Tri-State G & T Association Inc. | Barry Ingold | | |
| 5 | U.S. Army Corps of Engineers Northwestern Division | Karl Bryan | Affirmative | |
| 5 | U.S. Bureau of Reclamation | Martin Bauer | Negative | View |
| 5 | Wisconsin Electric Power Co. | Linda Horn | Negative | View |
| 5 | Wisconsin Public Service Corp. | Leonard Rentmeester | | |
| 6 | AEP Marketing | Edward P. Cox | Negative | View |
| 6 | Black Hills Corp | Tyson Taylor | | |
| 6 | Bonneville Power Administration | Brenda S. Anderson | Negative | View |
| 6 | Cleco Power LLC | Matthew D Cripps | Abstain | |
| 6 | Consolidated Edison Co. of New York | Nickesha P Carrol | Affirmative | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 6 | Constellation Energy Commodities Group | Chris Lyons | Affirmative | |
| 6 | Dominion Resources, Inc. | Louis S Slade | Negative | View |
| 6 | Duke Energy Carolina | Walter Yeager | Affirmative | |
| 6 | Entergy Services, Inc. | Terri F Benoit | Negative | |
| 6 | Eugene Water & Electric Board | Daniel Mark Bedbury | | |
| 6 | Exelon Power Team | Pulin Shah | Affirmative | |
| 6 | FirstEnergy Solutions | Mark S Travaglianti | Negative | View |
| 6 | Florida Power & Light Co. | Silvia P Mitchell | Abstain | |
| 6 | Lakeland Electric | Paul Shipps | Negative | View |
| 6 | Lincoln Electric System | Eric Ruskamp | Affirmative | |
| 6 | Louisville Gas and Electric Co. | Daryn Barker | Abstain | |
| 6 | New York Power Authority | Thomas Papadopoulos | Negative | |
| 6 | Northern Indiana Public Service Co. | Joseph O'Brien | Affirmative | |
| 6 | Progress Energy | James Eckelkamp | Abstain | |
| 6 | PSEG Energy Resources & Trade LLC | James D. Hebson | Affirmative | View |
| 6 | Public Utility District No. 1 of Chelan County | Hugh A. Owen | Negative | |
| 6 | Salt River Project | Mike Hummel | | |
| 6 | Seattle City Light | Dennis Sismaet | Negative | View |
| 6 | Seminole Electric Cooperative, Inc. | Trudy S. Novak | Affirmative | |
| 6 | Southern California Edison Co. | Marcus V Lotto | | |
| 6 | Xcel Energy, Inc. | David F. Lemmons | | |
| 8 | Edward C Stein | Edward C Stein | Affirmative | |
| 8 | James A Maenner | James A Maenner | Affirmative | |
| 8 | JDRJC Associates | Jim D. Cyrulewski | Negative | |
| 8 | Network & Security Technologies | Nicholas Lauriat | Affirmative | |
| 8 | Roger C Zaklukiewicz | Roger C Zaklukiewicz | | |
| 8 | Volkmann Consulting, Inc. | Terry Volkmann | | |
| 8 | Wally Magda | Wally Magda | Affirmative | |
| 9 | California Energy Commission | William Mitchell Chamberlain | Negative | View |
| 9 | Commonwealth of Massachusetts Department of Public Utilities | Donald E. Nelson | Negative | |
| 9 | Maine Public Utilities Commission | Jacob A McDermott | Abstain | |
| 9 | National Association of Regulatory Utility Commissioners | Diane J. Barney | | |
| 9 | Oregon Public Utility Commission | Jerome Murray | Negative | View |
| 9 | Utah Public Service Commission | Ric Campbell | Affirmative | |
| 10 | Electric Reliability Council of Texas, Inc. | Kent Saathoff | Negative | View |
| 10 | Midwest Reliability Organization | Dan R. Schoenecker | | |
| 10 | New York State Reliability Council | Alan Adamson | Affirmative | |
| 10 | Northeast Power Coordinating Council, Inc. | Guy V. Zito | Affirmative | |
| 10 | ReliabilityFirst Corporation | Jacquie Smith | Affirmative | |
| 10 | SERC Reliability Corporation | Carter B Edge | Affirmative | |
| 10 | Southwest Power Pool Regional Entity | Stacy Dochoda | | |
| 10 | Western Electricity Coordinating Council | Louise McCarren | Negative | View |
| | | | | |

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
*Washington Office:* 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2008 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Consideration of Comments

## Interpretation of CIP-004-1 by WECC (Project 2009-26)

The Interpretation of CIP-004-2 Drafting Team thanks all commenters who submitted comments on the interpretation of CIP-004-1 – Cyber Security – Personnel & Training, Requirement R2, R3, and R4, for WECC. This interpretation was posted for a 10-day initial ballot from January 6, 2010 – January 19, 2010. Stakeholders were asked to provide feedback on the interpretation and associated documents through an electronic comment system. There were 80 sets of comments, including comments from approximately 80 different people from approximately 53 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

**The Industry Segments are:**

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

| Voter | Entity | Segment |
|---|---|---|
| Rick Spyker | AltaLink Management Ltd. | 1 |
| Kirit S. Shah | Ameren Services | 1 |
| Jason Shaver | American Transmission Company, LLC | 1 |
| Donald S. Watkins | Bonneville Power Administration | 1 |
| Tony Kroskey | Brazos Electric Power Cooperative, Inc. | 1 |
| Paul Rocha | CenterPoint Energy | 1 |
| Robert Martinko | FirstEnergy Energy Delivery | 1 |
| Harold Taylor, II | Georgia Transmission Corporation | 1 |
| Ronald D. Schellberg | Idaho Power Company | 1 |
| Larry E Watt | Lakeland Electric | 1 |
| Terry Harbour | MidAmerican Energy Co. | 1 |
| John Canavan | NorthWestern Energy | 1 |
| Richard J. Kafka | Potomac Electric Power Co. | 1 |
| Kenneth D. Brown | Public Service Electric and Gas Co. | 1 |
| Tim Kelley | Sacramento Municipal Utility District | 1 |
| Robert Kondziolka | Salt River Project | 1 |
| Pawel Krupa | Seattle City Light | 1 |
| Richard Salgo | Sierra Pacific Power Co. | 1 |
| Dana Cabbell | Southern California Edison Co. | 1 |
| Horace Stephen Williamson | Southern Company Services, Inc. | 1 |
| Keith V. Carman | Tri-State G & T Association Inc. | 1 |
| John Tolo | Tucson Electric Power Co. | 1 |

| | | |
|---|---|---|
| Chuck B Manning | Electric Reliability Council of Texas, Inc. | 2 |
| Kim Warren | Independent Electricity System Operator | 2 |
| Kathleen Goodman | ISO New England, Inc. | 2 |
| Jason L Marshall | Midwest ISO, Inc. | 2 |
| Alden Briggs | New Brunswick System Operator | 2 |
| Gregory Campoli | New York Independent System Operator | 2 |
| Bobby Kerley | Alabama Power Company | 3 |
| Thomas R. Glock | Arizona Public Service Co. | 3 |
| Rebecca Berdahl | Bonneville Power Administration | 3 |
| Linda R. Jacobson | City of Farmington | 3 |
| Russell A Noble | Cowlitz County PUD | 3 |
| Jalal (John) Babik | Dominion Resources, Inc. | 3 |
| Joanne Kathleen Borrell | FirstEnergy Solutions | 3 |
| Leslie Sibert | Georgia Power Company | 3 |
| R Scott S. Barfield-McGinnis | Georgia System Operations Corporation | 3 |
| Gwen S Frazier | Gulf Power Company | 3 |
| Don Horsley | Mississippi Power | 3 |
| Terry L Baker | Platte River Power Authority | 3 |
| Jeffrey Mueller | Public Service Electric and Gas Co. | 3 |
| Kenneth R. Johnson | Public Utility District No. 1 of Chelan County | 3 |
| Greg Lange | Public Utility District No. 2 of Grant County | 3 |
| James Leigh-Kendall | Sacramento Municipal Utility District | 3 |
| John T. Underhill | Salt River Project | 3 |
| Dana Wheelock | Seattle City Light | 3 |
| Ronald L Donahey | Tampa Electric Co. | 3 |
| James R. Keller | Wisconsin Electric Power Marketing | 3 |
| Gregory J Le Grave | Wisconsin Public Service Corp. | 3 |
| David Frank Ronk | Consumers Energy | 4 |
| Guy Andrews | Georgia System Operations Corporation | 4 |
| Douglas Hohlbaugh | Ohio Edison Company | 4 |
| John D. Martinsen | Public Utility District No. 1 of Snohomish County | 4 |

| | | |
|---|---|---|
| Mike Ramirez | Sacramento Municipal Utility District | 4 |
| Hao Li | Seattle City Light | 4 |
| Anthony Jankowski | Wisconsin Energy Corp. | 4 |
| Francis J. Halpin | Bonneville Power Administration | 5 |
| Alan Gale | City of Tallahassee | 5 |
| James B Lewis | Consumers Energy | 5 |
| Mike Garton | Dominion Resources, Inc. | 5 |
| Kenneth Dresner | FirstEnergy Solutions | 5 |
| Gary L Tingley | Portland General Electric Co. | 5 |
| David Murray | PSEG Power LLC | 5 |
| Thomas J. Bradish | RRI Energy | 5 |
| Bethany Wright | Sacramento Municipal Utility District | 5 |
| Glen Reeves | Salt River Project | 5 |
| Michael J. Haynes | Seattle City Light | 5 |
| Martin Bauer | U.S. Bureau of Reclamation | 5 |
| Linda Horn | Wisconsin Electric Power Co. | 5 |
| Edward P. Cox | AEP Marketing | 6 |
| Brenda S. Anderson | Bonneville Power Administration | 6 |
| Louis S Slade | Dominion Resources, Inc. | 6 |
| Mark S Travaglianti | FirstEnergy Solutions | 6 |
| Paul Shipps | Lakeland Electric | 6 |
| James D. Hebson | PSEG Energy Resources & Trade LLC | 6 |
| Dennis Sismaet | Seattle City Light | 6 |
| William Mitchell Chamberlain | California Energy Commission | 9 |
| Jerome Murray | Oregon Public Utility Commission | 9 |
| Kent Saathoff | Electric Reliability Council of Texas, Inc. | 10 |
| Louise McCarren | Western Electricity Coordinating Council | 10 |

**Consideration of Comments on Initial Ballot — Interpretation of CIP-004-1 by WECC (Project 2009-26)**

**Summary Consideration:**
Since the previously-posted interpretation, the Interpretation Drafting Team ("IDT") has considered all of the submitted comments, and revised the interpretation. In addition to revisions made to address issues identified by commenters, the team revised the interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. Consistent with the guidance in the Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

Many commenters disagreed with the previously-posted interpretation's statement that there is no effective way to provide escorted or supervised cyber access, and they further noted that it is possible to provide escorted cyber access. Other comments note that escorted or supervised cyber access should be allowed.

The IDT recognizes there may be tools that allow escorted cyber access. However, pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT must consider the words of the standard as written. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, the standard requires that all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support.

Additionally, the IDT does not believe the standard allows for escorted or supervised cyber access to cyber assets, but agrees that the standard does allow for escorted or supervised physical access to cyber assets, as explained in the revised interpretation language.

Some commenters expressed concern about limitations in emergency situations. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures.

Other commenters noted concern about the reference in the previously-posted interpretation to the FAQ document. The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an

approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access. Although WECC's Request for Interpretation was submitted on CIP-004-1, this interpretation is applicable to all subsequent versions of the standard in which the requirement language for which the interpretation was requested persists. The FAQ was written for Version 1 of the CIP standards and the language concerning authorized access has not been modified to conform to the changes made in subsequent versions.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Shrayshuen, at 404-446-2563 or at herb.shrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[2]

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Chuck B Manning | Electric Reliability Council of Texas, Inc. | 2 | Negative | "ERCOT disagrees with the statement that "there is no way to provide effective escorted or supervised cyber access". The remote terminal session capabilities (e.g.: WebEx, etc.) do provide the means for supervised or "escorted" logical access. There are many instances where an entity will have to seek support from a call center and utilize the capabilities of whoever is available for support at that time. With many of these call centers being globally located, it is not feasible to utilize a pre-determined list of support technicians who have been screened or trained as required. These support scenarios may not be of a severity for the organization to actually declare an emergency thus triggering the CIP-003-1 R3 requirement." |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language . As written, CIP-004 requires that all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |

[2] The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| David Murray | PSEG Power LLC | 5 | Affirmative | "PSEG agrees that background checks and training are appropriate those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed." |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Gary L Tingley | Portland General Electric Co. | 5 | Negative | 1. NERC needs to better define "authorized access". 2. Authorized access should not include temporary vendor support that is accomplished under the supervision of an authorized individual. |
| **Response**: Thank you for the comment. The interpretation language has been revised. The IDT also notes that any change to the standard or associated definitions, such as your comment concerning better defining "authorized access," is outside the scope of the interpretation process. Nonetheless, while the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Edward P. Cox | AEP Marketing | 6 | Negative | AEP agrees with the SDT's response to question #2 and believes that a similar response should have been provided to question #1 as well. Simply stated, as the SDT described in its first sentence, " . . . the ACE referenced in BAL-002-0 Requirement 4 is ACE as defined in BAL-001-0.1a Requirement 1 . . . " The requesting entity is seeking to have the SDT approve that their particular application of an "adjusted ACE" for the standard is compliant. AEP believes that the definition of ACE, as defined in BAL-001-0.1a R1, provides for adjustments by the ADI as a pseudo-tie falling in the Net Interchange value and by time correction falling in the Frequency Schedule value. In response to the interpretation request, the SDT introduced an equivalent "reporting ACE" term that is not contained within the referenced standard requirements. The SDT then explains the |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | use of an ACE Diversity Interchange (ADI) in the context of a Reserve Sharing Group (RSG). The use of a new term and the subsequent ADI/RSG discussion modifies the standard requirements by interpretation, which is not consistent with the use of a request for interpretation. |
| **Response**: The IDT believes that this comment was intended for a different interpretation's posting and is outside the scope of this interpretation. | | | | |
| Jason Shaver | American Transmission Company, LLC | 1 | Negative | ATC appreciates the work of the standards drafting team but disagrees with the proposed interpretation. It is our understanding that the requirements in question apply strictly to those individuals that are granted un-supervised access to a cyber asset or un-escorted physical access of a Critical Cyber Asset. We believe that there are acceptable protocols/ processes that can provide effective supervision of a person within a cyber asset and therefore disagree with the SDT opinion that ""...there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors...". If an entity has protocols/processes in regards to supervision of a person accessing a cyber asset electronically then CIP-004-1 Requirements 2, 3 and 4 would not be applicable to the person being supervised. ATC recommends the following interpretation: CIP-004-1 Requirement 2, 3 and 4 govern the actions of an entity in their dealings over persons with authorized cyber access or authorized unescorted physical access to Critical Cyber Asset(s). In so much that they grant a person un-supervised or un-escorted access to either portions of or all Critical Cyber Assets. These requirements do not apply to persons who are supervised / escorted while they are accessing a cyber asset electronically or physically. |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| concept or any words relating to “escorting” or “supervision” in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Brenda S. Anderson | Bonneville Power Administration | 6 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Donald S. Watkins | Bonneville Power Administration | 1 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Francis J. Halpin | Bonneville Power Administration | 5 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Rebecca Berdahl | Bonneville Power Administration | 3 | Negative | BPA believes that the Interpretation is not clearly written and provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. BPA also believes that it is not always reasonable for a vendor to complete the risk assessment and training as required by CIP-004-1 Requirement 2, so would therefore like the Interpretation to address more clearly what "authorized access" is. An example of our concern is when a Cisco technician must access the system for troubleshooting and repairs, NERC CIP training and background checks are unreasonably burdensome and would preclude timely and effective repairs. The drafting team's response contradicts the guidance in FERC Order 706, page 116, paragraph 432 as well as the "Frequently Asked Questions" for CIP-004-1, and we are very concerned with the drafting team's dismissal of previous NERC and FERC guidance. We believe that the interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

**Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to “physical access,” the concept or any words relating to “escorting” or “supervision” relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of “authorized access” in the requirement does not exclude vendor support.

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. | | | | |
| Bethany Wright | Sacramento Municipal Utility District | 5 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| James Leigh-Kendall | Sacramento Municipal Utility District | 3 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Mike Ramirez | Sacramento Municipal Utility District | 4 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |
| Tim Kelley | Sacramento Municipal Utility District | 1 | Negative | Concerns about the interpretation having not only significant negative effects on the industry, but also an adverse affect on the overall reliability of the Bulk Electric System. Specifically, if all vendors providing support are subject to the requirements of CIP-004-1 R2, R3, and R4 it will have an immediate and direct impact on the operations of IT systems. These systems would be exposed to a far greater reliability risk through lack of support than any potential security risk associated with vendor access in a supervised capacity. SMUD has concern that the identified interpretation could limit SMUD's ability to have technical support during complex system outages if only fully vetted vendors can be used. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. The IDT notes that this interpretation does not affect an entity's ability to fully vet a vendor pursuant to Requirements R2, R3, and R4. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures. | | | | |
| Terry Harbour | MidAmerican Energy Co. | 1 | Negative | Contrary to the interpretation, MidAmercian believes you can 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 |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | electronic access |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Kent Saathoff | Electric Reliability Council of Texas, Inc. | 10 | Negative | ERCOT disagrees with the statement that "there is no way to provide effective escorted or supervised cyber access". Remote terminal session capabilities (e.g.: WebEx, etc.) do provide the means for supervised or "escorted" logical access. There are many instances where an entity will have to seek support from a call center and utilize their capabilities. With many of these call centers being globally located, it is not feasible to utilize a pre-determined list of support technicians who have been screened or trained as required. These support scenarios may not be of a severity for the organization to actually declare an emergency thus triggering the CIP-003-1 R3 requirement. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Linda R. Jacobson | City of Farmington | 3 | Negative | FEUS thanks the drafting team for the interpretation, however, does not fully agree. FEUS SME's decided to vote No on this interpretation. The interpretation does not clarify "authorized access" as it applies to temporary support from vendors for cyber access. FEUS does not agree effective escorted or supervised cyber access cannot be accomplished in some circumstances; such as, an authorized individual working directly with temporary vendor support. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Douglas Hohlbaugh | Ohio Edison Company | 4 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |
| Joanne Kathleen Borrell | FirstEnergy Solutions | 3 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | support. |
| Kenneth Dresner | FirstEnergy Solutions | 5 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Mark S Travaglianti | FirstEnergy Solutions | 6 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |
| Robert Martinko | FirstEnergy Energy Delivery | 1 | Negative | FirstEnergy appreciates the hard work put forth by the CIP SAR team in developing an interpretation for a challenging question posed by WECC. From our review of the response to WECC's request, the interpretation is saying that those vendors who are physically escorted to CCA would not require training and background checks, but once a vendor is given electronic cyber access, regardless of whether that access is remote or on-site, they must have been trained and risk assessed per the requirements of CIP-004-1. FirstEnergy respectfully disagrees with the interpretation team's position that states "For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access ..." We believe that when a vendor is physically on-site and being monitored by FE personnel that escorted access should be permissible even when the vendor is permitted cyber access to the given asset. FE feels prudent steps can be taken in this regard without the need for documented cyber training and risk assessments. We concur with the team's position in regards to remote cyber access and that background checks, personnel verification and training is prudent for remote support. |
| **Response**: Thank you for your comment. The IDT agrees in part and respectfully disagrees in part. In response to comments, the interpretation | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| language has been changed. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Alan Gale | City of Tallahassee | 5 | Negative | I am voting no because the standard, as written, allows a 30 day or 90 day grace period to perform the PRA and Training. This provision is removed from Version 2, both have to be performed prior to granting access. An entity could allow access to CCA's and not have the PRA/training done and be compliant if the access is for less than 30-days. While I agree it is not desired, it is allowed as written. The next version does NOT allow it. The Interpretation process cannot be used to start "enforcing" the next version prior to its authorization and implementation dates. |
| **Response**: Thank you for your comment. While the original request for interpretation was of CIP-004-1, as you have noted, the 30- and 90-day periods were eliminated in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. The drafting team agrees that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. | | | | |
| John Tolo | Tucson Electric Power Co. | 1 | Negative | I respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, I disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. I believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. I am therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." I believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. I believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the IDT disagrees that "authorized access" does not apply to vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Tony Kroskey | Brazos Electric Power Cooperative, Inc. | 1 | Negative | In one part of the response it says "there is no way to provide effective escorted or supervised cyber access" without a PRA and training to ensure that actions of the vendor do not harm. However, even with a PRA and training you still cannot ensure this. This interpretation needs more work. |
| **Response**: Thank you for your comment. The IDT has revised the interpretation in response to comments and pursuant to the NERC Guidelines for | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Interpretation Drafting Teams. | | | | |
| Richard J. Kafka | Potomac Electric Power Co. | 1 | Affirmative | Issue is "escorted access" for cyber assets. Interpretation says that there can be escorted physical access, but there is no such thing as escorted cyber access. Everyone with cyber access, including vendors, must meet the training a background checks for the registered entity's cyber security policy. As difficult as this may be for vendors and their customers, that is no reason other than emergencies to grant an exception to those who may have cyber access. |
| **Response**: Thank you for your comment. The IDT agrees, as explained in the revised interpretation. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Richard Salgo | Sierra Pacific Power Co. | 1 | Negative | It does not appear that the Drafting Team added any clarity to the term "authorized access" with this interpretation. It is our belief that "authorized access" refers to the authorization of permanent, direct, and unsupervised access to critical cyber assets, and disagree with the assertion that there is no means to provide effective supervision of vendor access to CCA's. We are troubled by the apparent dismissal of guidance provided in the FAQ's, as these FAQ's are heavily relied upon by the industry to guide compliance activities and decisions. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude temporary or non-permanent access.<br><br>The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Jalal (John) Babik | Dominion Resources, Inc. | 3 | Negative | Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability. |
| Louis S Slade | Dominion Resources, Inc. | 6 | Negative | Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability. |
| Mike Garton | Dominion Resources, Inc. | 5 | Negative | Many support vendors do not assign specific technicians to specific clients and/or accounts. We therefore can't support this interpretation. We could support if it allowed 'supervised electronic' access in lieu of 'escorted physical' access. Failure to modify the interpretation could substantially elongate repair time, which could have an adverse impact on reliability. |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude support vendors. | | | | |
| Alden Briggs | New Brunswick System Operator | 2 | Negative | NBSO is voting 'no' due to the physical access issue. Pertaining to physical access, NBSO believes that a person who is escorted by someone that has authorized access (PRA and cyber training) does not need the training. Pertaining to electronic access, NBSO believes all personal that have electronic access need to be trained. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| **Response**: Thank you for your comment. The IDT agrees as explained in the revised interpretation. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| James D. Hebson | PSEG Energy Resources & Trade LLC | 6 | Affirmative | PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non-emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed. |
| Jeffrey Mueller | Public Service Electric and Gas Co. | 3 | Affirmative | PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed. |
| Kenneth D. Brown | Public Service Electric and Gas Co. | 1 | Affirmative | PSEG agrees that background checks and training are appropriate for those electronically entering an ESP in typical situations. Emergency situations may require confirmation of background checks or distribution of training to be waived, but sessions should still be at least monitored. PSEG also agrees that the use of a monitored session for non emergency troubleshooting/operations and maintenance work, such as WebEx, could be acceptable, providing proper background checks and training are confirmed. |
| **Response:** Thank you for your comment. The IDT agrees in part and respectfully disagrees in part. In response to comments and pursuant the NERC's Guidelines for Interpretation Drafting Teams, the interpretation language has been changed. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. The IDT notes that the scope of this interpretation does not limit an | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| entity's emergency response procedures. | | | | |
| Russell A Noble | Cowlitz County PUD | 3 | Negative | Requirement for vendors to submit to each entity's Risk Assessment and Cyber Training program appears not workable. Once an entity finds a vendor not cooperative, what then? When buying new equipment, vendors are more cooperative. But for older equipment/software there is not much incentive to induce vendors to comply. This forces the entity in a very hard position. |
| **Response**: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. | | | | |
| Dana Wheelock | Seattle City Light | 3 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Dennis Sismaet | Seattle City Light | 6 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003- |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | 1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. Thank you. |
| Hao Li | Seattle City Light | 4 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Michael J. Haynes | Seattle City Light | 5 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Pawel Krupa | Seattle City Light | 1 | Negative | Seattle City Light respectfully disagrees with the proposed interpretation because it does not directly answer the questions raised by WECC. In addition, the interpretation provides a circular definition by using the very term ("authorized access") WECC sought to clarify. Furthermore, we disagree with the assertion that a utility cannot provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner balancing security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe "authorized access" refers to individuals permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electric industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are, therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but, in fact, provide valuable guidance and help to clarify the intent of the standards. We believe interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Paul Shipps | Lakeland Electric | 6 | Negative | Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Larry E Watt | Lakeland Electric | 1 | Negative | supervised cyber access is possible and manageable by any able cyber security team and should not require the time and expense of training vendors for single access sessions. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. | | | | |
| Ronald L Donahey | Tampa Electric Co. | 3 | Negative | Tampa Electric thanks the Standards Drafting Team for the opportunity to comment during the Initial Ballot for the interpretation of Project 2009-26. , WECC Interpretation. We believe cyber escorting of personnel without specifically authorized access should be allowed without requiring a pre-screening via the Personnel Risk Assessment and pre-NERC training as in a network operation center support arrangement. The support vendors cannot always guarantee the availability of specific support personnel during an emergency or unplanned situation. This leaves a utility in position of potential violation versus a potential reliability issue if this is not resolved. Tampa Electric proposes that NERC establish some type of vendor certification program for the sector that would allow major systems vendors (such as Areva, GE, Emerson,Cisco, etc.) to certify at the energy sector level that they meet the Personnel Risk Assessment and training requirements so that each utility does not need to perform this for personnel who are working throughout the industry for multiple entities. It the interpretation of the drafting team as currently worded is adopted, then we suggest that the certification program be developed first so that vendors can certify to NERC that they meet the requirements which would allow them to be certified for utility purposes. It is our position that the Standards Drafting Team has not sufficiently addressed the question raised by WECC on the supervision or escorted cyber access. Based on these factors, Tampa Electric votes no to the adoption of this interpretation. |
| **Response**: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| James B Lewis | Consumers Energy | 5 | Negative | The interpretation seems to make the determination that there is “no way to provide effective escorted or supervised cyber access”. Thus, anyone granted any type of cyber access to a critical cyber asset must be compliant with CIP-004 R2, R3 and R4. Our Subject Matter Experts believe that there are acceptable protocols that can provide effective supervision of a person accessing critical cyber assets. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to “physical access,” the concept or any words relating to “escorting” or “supervision” relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Bobby Kerley | Alabama Power Company | 3 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | employee at all and this would be considered compliant. But if we don't train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |
| Don Horsley | Mississippi Power | 3 | Negative | The interpretation states "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. " We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement "...there is no way to provide...". This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don't train and |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |
| Gwen S Frazier | Gulf Power Company | 3 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don’t train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Horace Stephen Williamson | Southern Company Services, Inc. | 1 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement “...there is no way to provide...”. This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don’t train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |
| Leslie Sibert | Georgia Power Company | 3 | Negative | The interpretation states “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. “ We believe that statements concerning available technology at a point in time should not be made in the context of a NERC standard |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | interpretation. The interpretation will be binding and it is a lengthy process to change once approved. We therefore disagree with the statement "...there is no way to provide...". This interpretation specifically invalidates the Webex concept used for vendor support where an authorized employee logs onto the system that needs vendor support and sets up a WebEx session the vendor can attach to and remotely control the mouse/keyboard. The employee can monitor everything the vendor is doing and if the employee disconnect the session at any time. This solution provides a vendor remote support session that MUST be initiated by the employee otherwise the vendor has no access; we have the employee watching what the vendor does and can instantly disconnect all their access; and we can have auditing and logging/recording of the entire session. In our view, that is a better controlled situation than if the vendor came to physically work on the equipment and was physically escorted where the escort would have to shoulder-surf to see what is actually occurring on the system. This interpretation instead states that as long as we run the vendor through a training program and verify their SSN and 7 year criminal background, we can let them do whatever, whenever, however they would like remotely with no involvement from an employee at all and this would be considered compliant. But if we don't train and background check them, but instead we initiate a session with them and watch their every move on our systems, we're non-compliant. The interpretation even acknowledges that this is in opposition to the CIP FAQ document. |

**Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude temporary or non-permanent access.

The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| modified to eliminate the need for the interpretation. | | | | |
| Paul Rocha | CenterPoint Energy | 1 | Negative | The SAR Drafting team indicated the FAQ document should not be relied upon for guidance in this case. CenterPoint Energy does not agree that an interpretation should replace previously published documents intended to guide entities in their compliance efforts. The disagreement between the FAQ document and the SAR Drafting team's interpretation creates confusion and therefore CenterPoint Energy must submit a negative vote. |
| **Response**: Thank you for the comment. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Kim Warren | Independent Electricity System Operator | 2 | Negative | The scenario that WECC is concerned with presents a situation where it is quite likely that emergency support personnel would not be granted authorized access but would conduct their work using an account that has been authorized to the person who is required to escort or “supervise” the work being done under the account. The authorized owner of the account would be responsible, and in fact liable, for all activities that occur using that account. This places the onus on the account owner not the emergency support personnel which in turn places the requirement for training and PRA on the account owner not the emergency support personnel. The emergency support personnel are not being granted authorized access but are allowed the supervised use of an account that has been authorized to somebody else. NERC CIP-004-1 R2,R3 refer to authorized access as the determining factor for the requirement of training and Personnel Risk Assessment. As the situation for which WECC is seeking clarification contemplates a situation where, in all likelihood, authorized access would not be granted, therefore training and a PRA are not required. The interpretation that is presented does not contemplate this situation and therefore does not provide an |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | appropriate or complete interpretation. It is suggested that the interpretation be revised to reflect the scenario as described. |
| **Response**: Thank you for the comment. While the IDT appreciates this concern, it must develop its interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors. The IDT notes that the scope of this interpretation does not limit an entity's emergency response procedures. | | | | |
| Gregory J Le Grave | Wisconsin Public Service Corp. | 3 | Negative | The standard should allow the escorted cyber access. It is the responsibility of the entity to assure that the escorting can detect malicious behavior. Failure to implement adequate controls would be a violation of the standard. |
| **Response**: The IDT is limited by the Guidelines for Interpretation Drafting Teams to clarify the meaning of the standard, not to expand the reach of the standard. While the IDT appreciates the comment, any change of the standard is outside the scope of the interpretation process. | | | | |
| Anthony Jankowski | Wisconsin Energy Corp. | 4 | Negative | There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| James R. Keller | Wisconsin Electric Power Marketing | 3 | Negative | There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel. |
| Linda Horn | Wisconsin Electric Power Co. | 5 | Negative | There are tools available that do allow escorted cyber access to CCA's making this interpretation of the standard false. The original standard was written in a broader sense to include escorted cyber access. Providing evidence of compliance would be difficult if not impossible for certain situations such as local assistance from support personnel. |
| **Response**: Thank you for the comment. The interpretation language has been revised. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. Local assistance from support personnel must be managed as authorized cyber access, authorized unescorted physical access, or through visitor management programs, and this interpretation does not change requirements for compliance evidence. | | | | |
| Greg Lange | Public Utility District No. 2 of Grant County | 3 | Negative | This interpretation does not answer the second part of Question one and therefore does not lend any clarity to the requested interpretation. |
| **Response**: Thank you for the comment. The interpretation language has been revised. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Guy Andrews | Georgia System Operations Corporation | 4 | Negative | We are in agreement with the following comments provided by WECC: We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | FERC. |
| Harold Taylor, II | Georgia Transmission Corporation | 1 | Negative | We are in agreement with the following comments provided by WECC: We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| David Frank Ronk | Consumers Energy | 4 | Negative | We concur with the comments provided by ATC |
| **Response**: Thank you for the comment. The interpretation language has been revised. Pursuant to the NERC Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Jason L Marshall | Midwest ISO, Inc. | 2 | Negative | We disagree with ignoring the FAQ that was developed by the standards drafting team. It gives insight into the intent of the SDT when developing the standard. The FAQ clearly considers cyber escorting possible. We do not think the drafting team should prevent creative solutions that may allow cyber escorting since the standard does not specifically exclude it. Further, the interpretation seems to imply that the background check must be completed prior to granting access. The standard is clear that any background checks can be completed up to 30 days after the access is granted. |
| **Response**: Thank you for the comment. The interpretation language has been revised, and the IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Kathleen Goodman | ISO New England, Inc. | 2 | Negative | We disagree with the interpretation, as stated. The standard does allow for escorted/ supervised access to cyber assets for both logical and physical. However, if a company allowed external logical access the individual would need to meet the standard. If the individual is physically on site and is given logical access and is supervised by a qualified escort this is allowed. Therefore, we believe the Interpretation changes the existing Standard. Further, the statement by the SDT that "It is further noted that an FAQ is not a standard, and cannot create or dilute the language of the standard itself." seems to support the argument for expansion of the requirements since the FAQs, historically, have been used extensively by the industry to develop a voting position on Standards. This Interpretation appears to change the information the industry had available to it at the time the Standard was adopted. |
| **Response**: Thank you for your comment. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| R3, and R4.<br><br>The IDT has further clarified the limited reference to the FAQ. The FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1 of CIP-004—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions of CIP-004. Because the issue for which WECC requested clarification persists in subsequent versions of CIP-004, this interpretation will be applicable to all approved versions of CIP-004 until a version is approved in which the requirement language is modified to eliminate the need for the interpretation. | | | | |
| Kirit S. Shah | Ameren Services | 1 | Negative | We do not agrre with the interpretation. With this interpretation if a Technician from a vendor was physically escorted inside the ESP he/she would not be allowed to work on any CCA's unless he had training and background check even though he is physically escorted. This could impact operations and potentially the operation of the BES. |
| **Response**: Thank you for the comment. The interpretation language has been revised. The IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. | | | | |
| Dana Cabbell | Southern California Edison Co. | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Glen Reeves | Salt River Project | 5 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Gregory Campoli | New York Independent System Operator | 2 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, we disagree with the assertion that there is no way to provide effective supervision of cyber access to ensure actions do not harm the integrity of the Critical Cyber Asset or the reliability of the bulk power system. Finally, we are concerned about the reversal of previous NERC and FERC guidance. The interpretation does not directly answer the questions raised by WECC. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that is accomplished by an authorized individual working with the vendor in a supervising |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. We disagree with the assertion that there is no way to provide effective supervision of cyber access. There are tools available which can enable authorized personnel to provide temporary, indirect and monitored cyber access to personnel who have not been subjected to a personnel risk assessment and training. Furthermore, such tools can enable the supervising personnel to immediately revoke such access as needed. Therefore, we believe it is possible to provide supervised cyber access which can be controlled at least as effectively as escorted physical access. Finally, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Jerome Murray | Oregon Public Utility Commission | 9 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| John Canavan | NorthWestern Energy | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| John D. Martinsen | Public Utility District No. 1 of Snohomish County | 4 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| John T. Underhill | Salt River Project | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Keith V. Carman | Tri-State G & T Association Inc. | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| R Scott S. Barfield-McGinnis | Georgia System Operations Corporation | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| Rick Spyker | AltaLink Management Ltd. | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Robert Kondziolka | Salt River Project | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Ronald D. Schellberg | Idaho Power Company | 1 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Terry L Baker | Platte River Power Authority | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Thomas J. Bradish | RRI Energy | 5 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Thomas R. Glock | Arizona Public Service Co. | 3 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| William Mitchell Chamberlain | California Energy Commission | 9 | Negative | We respectfully disagree with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, we disagree with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. We are therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." We believe that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. We believe that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Kenneth R. Johnson | Public Utility District No. 1 of Chelan County | 3 | Negative | WECC comments apply |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |
| Louise McCarren | Western Electricity Coordinating Council | 10 | Negative | WECC respectfully disagrees with the interpretation provided by the Cyber Security Order 706 SAR drafting team because it does not directly answer the questions raised by WECC. In addition, the drafting team's interpretation provides a circular definition by using the very term ("authorized access") that WECC sought to clarify. Furthermore, WECC disagrees with the assertion that there is no way to provide adequate supervision of vendor support in all circumstances. Providing supervised access when an individual does not require permanent or extended access to a system is a security "best practice". Supervised support can be provided in a manner that balances security risks with operational risks associated with not having timely and accessible vendor support of critical systems. The drafting team should clarify how it defines the term "authorized access" as it applies to vendors providing temporary support. WECC believes that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| | | | | only by an authorized individual working with the vendor in a supervising capacity. In other words, temporary, supervised vendor support is distinguishable from and not included in the definition of the term "authorized access" as it is used in the relevant CIP reliability standards. Additionally, the mention of CIP-003-1 R3 for exemptions from an entity's cyber security policy adds no clarity to the interpretation. In fact, it may cause further confusion by leading entities to believe that they can exempt themselves from the requirements of a standard. If the drafting team feels compelled to refer to CIP-003-1 Requirement R3, the reference should be carefully detailed to avoid potential confusion. In addition, many entities in the electricity industry have relied on the NERC FAQs and statements by FERC in Order 706 to understand the intent of the standards. WECC is therefore, extremely concerned by the drafting team's dismissal of previous NERC and FERC guidance embodied in their responses that, "..... this particular guidance should be revisited" and, ".....an FAQ is not a standard, and cannot create or dilute the language of the standard itself." WECC believes that neither the FAQs, nor FERC Order 706 initially approving the CIP reliability standards, dilute the language of the standards but in fact, provide valuable guidance and help to clarify the intent of the standards. WECC believes that interpretations should seek to clarify the intent of a standard while remaining consistent with the guidance and statements of NERC and FERC. |
| **Response**: The IDT thanks you for your comment. The interpretation language has been revised, which addresses many of the concerns in your comments. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. For the same reason, the scope of "authorized access" in the requirement does not exclude vendors providing temporary support. The IDT has removed the reference in the interpretation to CIP-003, R3, and has further clarified the limited reference to the FAQ. | | | | |

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| Martin Bauer | U.S. Bureau of Reclamation | 5 | Negative | While the SDT may have answered the questions, the response is not of the quality that can be used for reference and should be revised. There were two questions asked in this request for interpretation: 1. Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? 2. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? The response to the first question was "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." The response indicates that vendors must be authorized. Although not referenced directly it can be inferred that the response to the second questions was "....For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access....." This response is not framed well. If the inference is correct it appears to be consistent with Standard. The WECC interpretation is not consistent with the Standard. It is clear from the standards that no person can be granted permanent access and WECC is also correct that there is no standard provision for vendor temporary access except under an emergency. This does not change the response to the request for interpretation. The response is sound if it is true that there is no way to supervise cyber access as was Toni's response. "There is no such thing as escorted cyber access. I think careful reading of the standard supports that interpretation. " WECC's response in question is "We believe that "authorized access" refers to individuals that are permanently authorized for direct, unsupervised access to cyber assets. Correspondingly, "authorized access", as used in the standard, does not include temporary vendor support that can be accomplished only by an authorized individual working with the vendor in a supervising capacity." |

**Response**: Thank you for the comment. The interpretation language has been revised. The IDT does not believe the standard allows for escorted/supervised cyber access to cyber assets, but agrees that the standard does allow for escorted/supervised physical access to cyber assets, as explained in the revised interpretation language. While the IDT recognizes there may be tools that allow escorted cyber access, compared to "physical access," the concept or any words relating to "escorting" or "supervision" relative to cyber access is absent from the requirement language. As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3,

| Voter | Entity | Segment | Vote | Comment |
|---|---|---|---|---|
| and R4. For the same reason, the scope of “authorized access” in the requirement does not exclude vendors providing temporary support. | | | | |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Note: an Interpretation cannot be used to change a standard.**

| Request for an Interpretation of a Reliability Standard |
|---|
| Date submitted: 10/15/09 |
| Date accepted: 10/23/09 |
| **Contact information for person requesting the interpretation:** |
| Name: John Van Boxtel |
| Organization: Western Electricity Coordinating Council |
| Telephone: 360-713-9090 |
| E-mail: jvanboxtel@wecc.biz |
| **Identify the standard that needs clarification:** |
| Standard Number: CIP-004-1 |
| Standard Title: Cyber Security – Personnel and Training |
| **Identify specifically what requirement needs clarification:** |

**Requirement Number and Text of Requirement:** R2, R3, and R4

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

**Clarification needed (emphasis added):**

Specifically, the WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would

temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

**Background**

Through previously published documents, both NERC and FERC have indicated that the intent of the CIP-004 Standard was to document training, risk assessment, and access to Critical Cyber Assets in situations where personnel have direct and unmonitored access to critical cyber assets, as opposed to and distinguishable from **supervised access.**

The question asked in Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training is: "*What is meant by 'authorized cyber access?'" The answer provided is:*

> *The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.* (emphasis added)

This answer is also consistent with a similar description of escorted access provided in FERC Order 706, page 116, paragraph 432, in which the Commission stated:

> *Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power system. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.* (emphasis added)

**Identify the material impact associated with this interpretation:**

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

**Material Impact**

If "Authorized Access" includes temporary support access provided in a supervised manner, then there is a potential for many Registered Entities to either be noncompliant while seeking support, or excessively burdened by limiting access to timely support. This situation is particularly likely from large non-utility vendors (such as Cisco Systems) that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard.

Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations:

- Training covering the specific policies, access controls, and procedures as developed by each individual Registered Entity.
- A personnel risk assessment for all support personnel provided by each individual vendor, based on the cyber security training program developed by each individual Registered Entity.
- Timely updates to each Registered Entity's access list of all support personnel provided by each individual vendor, including changes in personnel at the vendor within the timeframes prescribed by the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

## Project 2009-26: Response to Request for an Interpretation of NERC Standard CIP-004-1 for the Western Electricity Coordinating Council

The following interpretation of NERC Standard CIP-004-1 Cyber Security — Personnel & Training, Requirements R2, R3, and R4, was developed by the Cyber Security Order 706 SAR drafting team.

### Requirement Number and Text of Requirement

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

### Question

The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

### Response

WECC asks three questions, which are listed below. The answer to each question follows the question.

1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

   Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.

2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Note: an Interpretation cannot be used to change a standard.**

| Request for an Interpretation of a Reliability Standard |
|---|
| Date submitted: 10/15/09 |
| Date accepted: 10/23/09 |
| **Contact information for person requesting the interpretation:** |
| Name: John Van Boxtel |
| Organization: Western Electricity Coordinating Council |
| Telephone: 360-713-9090 |
| E-mail: jvanboxtel@wecc.biz |
| **Identify the standard that needs clarification:** |
| Standard Number: CIP-004-1 |
| Standard Title: Cyber Security – Personnel and Training |
| **Identify specifically what requirement needs clarification:** |

**Requirement Number and Text of Requirement:** R2, R3, and R4

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

**Clarification needed (emphasis added):**

Specifically, the WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would

temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

**Background**

Through previously published documents, both NERC and FERC have indicated that the intent of the CIP-004 Standard was to document training, risk assessment, and access to Critical Cyber Assets in situations where personnel have direct and unmonitored access to critical cyber assets, as opposed to and distinguishable from **supervised access.**

The question asked in Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training is: "*What is meant by 'authorized cyber access?'" The answer provided is:*

> *The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.* (emphasis added)

This answer is also consistent with a similar description of escorted access provided in FERC Order 706, page 116, paragraph 432, in which the Commission stated:

> *Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power system. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.* (emphasis added)

**Identify the material impact associated with this interpretation:**

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

**Material Impact**

If "Authorized Access" includes temporary support access provided in a supervised manner, then there is a potential for many Registered Entities to either be noncompliant while seeking support, or excessively burdened by limiting access to timely support. This situation is particularly likely from large non-utility vendors (such as Cisco Systems) that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard.

Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations:

- Training covering the specific policies, access controls, and procedures as developed by each individual Registered Entity.
- A personnel risk assessment for all support personnel provided by each individual vendor, based on the cyber security training program developed by each individual Registered Entity.
- Timely updates to each Registered Entity's access list of all support personnel provided by each individual vendor, including changes in personnel at the vendor within the timeframes prescribed by the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

## Project 2009-26: Response to Request for an Interpretation of NERC Standard CIP-004-1 for the Western Electricity Coordinating Council

The following interpretation of NERC Standard CIP-004-1 Cyber Security — Personnel & Training, Requirements R2, R3, and R4, was developed by the Cyber Security Order 706 SAR drafting team.

### Requirement Number and Text of Requirement

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

### Question

The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

### Response

~~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.~~

WECC asks three questions, which are listed below. The answer to each question follows the question.

1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.

2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

## A. Introduction

**1. Title:** Cyber Security — Personnel & Training

**2. Number:** CIP-004-3

**3. Purpose:** Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

**4. Applicability:**

**4.1.** Within the text of Standard CIP-004-3, "Responsible Entity" shall mean:

**4.1.1** Reliability Coordinator.

**4.1.2** Balancing Authority.

**4.1.3** Interchange Authority.

**4.1.4** Transmission Service Provider.

**4.1.5** Transmission Owner.

**4.1.6** Transmission Operator.

**4.1.7** Generator Owner.

**4.1.8** Generator Operator.

**4.1.9** Load Serving Entity.

**4.1.10** NERC.

**4.1.11** Regional Entity.

**4.2.** The following are exempt from Standard CIP-004-3:

**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.3** Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

**5. Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

**R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

**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:

**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.

## C. Measures

**M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

**M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

**M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

**M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

**1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

**1.1.2** ERO for Regional Entity.

**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### 1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

**1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.5. Additional Compliance Information

### 2. Violation Severity Levels (To be developed later.)

## E. Regional Variances

None identified.

### Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 01/16/06 | D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…" | 03/24/06 |
| 1 | 06/01/06 | D.2.1.4 — Change "access control rights" to "access rights." | 06/05/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Reference to emergency situations.<br>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.<br>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.<br>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".<br>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Update version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by NERC Board of Trustees | Update |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Unofficial Comment Form
## Project 2009-26 Interpretation of CIP-004-1 for the Western Electricity Coordinating Council

Please **DO NOT** use this form to submit comments. Please use the electronic comment form located at the link below to submit comments on the Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (Project 2009-26). The electronic comment form must be completed by **March 23, 2012.**

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

If you have questions please contact Steven Noess at steven.noess@nerc.net or by telephone at (404) 446-9691.

### Background Information

An initial ballot for this interpretation closed on January 19, 2010, with a quorum of 84.21% and an approval of 42.24%. Since that date, a project team from the CIP Interpretation Drafting Team ("IDT") has reviewed and responded to the comments received from that posting and made revisions to the interpretation of WECC's Request for Interpretation. The project team revised the interpretation pursuant to the NERC Guidelines for Interpretation Drafting Teams. In consideration of the Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

In their Request for Interpretation, WECC asked for clarity on the definition of "authorized access" as applied to temporary support from vendors. WECC also asks whether the requirements specified in CIP-004-1, R2, R3, and R4, apply to vendors who are supervised, whether by remote terminal access or escorted physical access.

The IDT determined that, as written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.The IDT recognizes there may be tools that allow escorted cyber access, but compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

In response to the portion of WECC's question related to "supervision," the IDT does not believe the standard allows for escorted or supervised cyber access to cyber assets, but agrees that the standard does allow for escorted or supervised physical access to cyber assets, as explained in the revised interpretation language.

The IDT notes that it is limited in its response to a request for interpretation to the clarification that it has provided. The interpretation drafting team must consider the request for interpretation within the confines of the NERC "Guidelines for Interpretation Drafting Teams," and it realizes that in some cases, some entities may not desire the outcome of this interpretation. However, it is not the role of an IDT to change a Reliability Standard or its applicability through an interpretation. The team understands that some may disagree with the outcome of this interpretation, and it notes that the greater standards development process is better equipped to weigh those concerns, if any. Revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Furthermore, an interpretation is limited and may not "address a gap or perceived weakness in the approved Reliability Standard[.]"

**You do not have to answer all questions. Enter All Comments in Simple Text Format.**

*Insert a "check" mark in the appropriate boxes by double-clicking the gray areas.*

Please review the request for an interpretation, the associated standard, and the draft interpretation and then answer the following questions.

1. The NERC Board of Trustees indicated that the interpretation process **should not** be used to address requests for a decision on **"how"** a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?

   ☐ The request is asking for clarity on the **meaning** of a requirement.

   ☐ The request is asking for clarity on the **application** of a requirement.

   Comments:

2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?

   ☐ The interpretation expands the reach of the standard.

   ☐ The interpretation does not expand the reach of the standard.

   Comments:

3. Do you agree with this interpretation? If not, please explain specifically what you disagree with.

   ☐ Yes

   ☐ No

   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Project 2009-26 Interpretation of CIP-004-x for WECC

## Project 2010-INT-05 Interpretation of CIP-002-x for Duke

**Two Ballot Windows (One Initial and One Successive)**
**Now Open Through 8 p.m. Eastern Friday, March 23, 2012**

**Now Available: Project 2009-26 | Project 2010-INT-05**

The following ballot windows for two CIP interpretations are now open: 1) an initial ballot window for an interpretation of standard CIP-002-x — Critical Cyber Asset Identification, Requirements R3, and 2) a successive ballot window for an interpretation of standard CIP-004-x — Cyber Security — Personnel & Training, Requirements R2, R3, and R4, for WECC. Both ballot windows are open **until 8 p.m. EST on Friday, March 23, 2012.**

### Instructions for Balloting on the Interpretations of CIP-002-x for Duke and CIP-004-x for WECC

Members of the ballot pools associated with each of these interpretations may log in and submit their votes for the interpretations by clicking here.

### Special Instructions for Submitting Comments with a Ballot

Please note that each interpretation has a separate electronic comment form, and for each interpretation, comments submitted during the formal comment period and the ballot for the interpretation use the same electronic form. It is NOT necessary for ballot pool members to submit comments through the ballot application – **all comments should be submitted through the electronic comment form associated with the interpretation**.

### Next Steps

The drafting team will consider all comments submitted to determine whether to make additional revisions to the interpretation.

### Background

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team and assigned the further development of all outstanding CIP Interpretations, including the two referenced in this announcement, to that team. Initial drafts of each of the two CIP interpretations were developed by a different drafting team. The CIP Interpretation Drafting Team has reviewed all comments submitted in the previous postings of each interpretation, along with FERC orders issued since the previous posting,

and has revised the interpretations in response to comments and consistent with guidance adopted by the NERC Board of Trustees and Standards Committee.

Information about the CIP Interpretation Drafting team is available on the team's webpage, which contains links to each of the interpretations that the team is working on including the two being balloted now.

**Standards Development Process**

The Standard Processes Manual contains all the procedures governing the standards development and interpretation processes. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

*For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.*

North American Electric Reliability Corporation
3353 Peachtree Rd NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Project 2009-26 Interpretation of CIP-004-x for WECC

## Project 2010-INT-05 Interpretation of CIP-002-x for Duke

Two Ballot Pool Windows Now Open through 8 a.m. Eastern on March 8, 2012
Two Formal Comment Periods Open through Friday 8 p.m. March 23, 2012
Two Ballot Windows (One Initial and One Successive) Open March 14 – 23, 2012

**Now Available Here:**

**Project 2010-INT-05 CIP-002-x Interpretation of CIP-002-x for Duke**
**Project 2009-26 Interpretation of CIP-004-x for WECC**

The CIP Interpretation Drafting team has posted two CIP Interpretations for formal comment periods through 8 p.m. Eastern on Friday, March 23, 2012. Ballot pools are being formed for each interpretation through **8 a.m. Eastern on Thursday, March 8** (*please note that ballot pools close at 8 a.m. on the day they close*). Ballots of each interpretation will be conducted during the last ten days of the comment period, from Wednesday, March 14 through Friday, March 23, 2012, closing at 8 p.m. Eastern.

**Instructions for Joining Ballot Pools**

Separate ballot pools are being formed for each interpretation. Although a ballot pool was previously formed for Project 2009-26, the Standards Committee has authorized forming a new ballot pool to ensure that current Registered Ballot Body members have an opportunity to participate.

To join the ballot pools to be eligible to vote in the upcoming ballots of each interpretation, go to: Join Ballot Pool

During the pre-ballot windows, members of each ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) One ballot pool list server has been set up and can be used for communication on each of the interpretations.

**The list servers for each interpretation project are:**

Project 2009-26 Interpretation of CIP-004-x for WECC: bp-2009-26_CIP-004-1_SB_in@nerc.com

Project 2010-INT-05 Interpretation of CIP-002-x for Duke Energy bp-2010-INT-05_CIP-002_in@nerc.com

## Instructions for Commenting

A formal comment period is open for each interpretation through **8 p.m. Eastern on Friday, March 23, 2012**. Each interpretation has a separate comment form. Please use the links below to submit comments using the electronic comment form for each interpretation. Off-line, unofficial copies of the comment forms are posted on the project pages.

| | | |
|---|---|---|
| **Project 2010-INT-05 Interpretation of CIP-002-x for Duke** | Electronic comment form | Project page |
| **Project 2009-26 Interpretation of CIP-004-x for WECC** | Electronic comment form | Project page |

If you experience any difficulties in using the electronic forms, please contact Monica Benson at monica.benson@nerc.net.

## Next Steps

A successive ballot window will be open for the interpretation in Project 2009-26 Interpretation of CIP-004-x for WECC from Wednesday, March 14 through 8 p.m. Eastern on Friday, March 23, 2012.

An initial ballot window will be open for the interpretation in Project 2010-INT-05 Interpretation of CIP-002-x for Duke from Wednesday, March 14 through 8 p.m. Eastern on Friday, March 23, 2012.

## Background

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team and assigned the further development of all outstanding CIP Interpretations, including the two referenced in this announcement, to that team. Initial drafts of each of the two CIP interpretations were developed by a different drafting team. The CIP Interpretation Drafting Team has reviewed all comments submitted in the previous postings of each interpretation, along with FERC orders issued since the previous posting, and has revised the interpretations in response to comments and consistent with guidance adopted by the NERC Board of Trustees and Standards Committee.

Additional information about each project is available on the individual project pages:

**Project 2010-INT-05 Interpretation of CIP-002-x for Duke**
**Project 2009-26 Interpretation of CIP-004-x for WECC**

## Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

*For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.*

North American Electric Reliability Corporation
116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement
## Project 2009-26 Interpretation of CIP-004-x for WECC
## Project 2010-INT-05 Interpretation of CIP-002-x for Duke

### Initial and Successive Ballot Results

**Now Available** 2009-26|2010-INT-05

Ballots of two CIP interpretations concluded Friday, March 23, 2012:

- An initial ballot of Project 2009-26 – Interpretation of CIP-004-x for WECC
- A successive ballot of Project 2010-INT-05 – Interpretation of CIP-002-x for Duke

Voting statistics for each ballot are listed below, and the Ballots Results page provides a link to the detailed results.

| Standard | Quorum | Approval |
|---|---|---|
| Project 2009-26 Interpretation of CIP-004-x for WECC | Quorum: 88.55% | Approval: 79.61% |
| Project 2010-INT-05 Interpretation of CIP-002-x for Duke | Quorum: 89.63% | Approval: 94.71% |

**Next Steps**

The CIP Interpretation Drafting Team (CIP IDT) will consider all comments submitted for each interpretation, and based on the comments, for each interpretation will determine whether to make additional revisions to the interpretation. If the drafting team determines that no substantive changes to the interpretation are required to address the comments, a recirculation ballot of the interpretation will be conducted. If the drafting team decides to make substantive revisions to either interpretation, the drafting team will submit the revised interpretation and consideration of the comments received for a quality review prior to posting for a parallel formal 30-day comment period and successive ballot.

**Background**

In May 2011 the Standards Committee appointed a standing CIP Interpretation Drafting team, and assigned these interpretations to that team.

**Standards Development Process**

The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

*For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.*

## Ballot Results

| | |
|---|---|
| **Ballot Name:** | Project 2009-26 Successive Ballot CIP-004-1 WECC_in |
| **Ballot Period:** | 3/14/2012 - 3/23/2012 |
| **Ballot Type:** | Initial |
| **Total # Votes:** | 294 |
| **Total Ballot Pool:** | 332 |
| **Quorum:** | **88.55 % The Quorum has been reached** |
| **Weighted Segment Vote:** | 79.61 % |
| **Ballot Results:** | **The drafting team is considering comments.** |

### Summary of Ballot Results

| Segment | Ballot Pool | Segment Weight | Affirmative # Votes | Affirmative Fraction | Negative # Votes | Negative Fraction | Abstain # Votes | No Vote |
|---|---|---|---|---|---|---|---|---|
| 1 - Segment 1. | 85 | 1 | 51 | 0.75 | 17 | 0.25 | 10 | 7 |
| 2 - Segment 2. | 10 | 0.7 | 7 | 0.7 | 0 | 0 | 2 | 1 |
| 3 - Segment 3. | 78 | 1 | 50 | 0.746 | 17 | 0.254 | 3 | 8 |
| 4 - Segment 4. | 23 | 1 | 15 | 0.882 | 2 | 0.118 | 3 | 3 |
| 5 - Segment 5. | 74 | 1 | 35 | 0.673 | 17 | 0.327 | 10 | 12 |
| 6 - Segment 6. | 46 | 1 | 26 | 0.722 | 10 | 0.278 | 5 | 5 |
| 7 - Segment 7. | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 - Segment 8. | 8 | 0.6 | 5 | 0.5 | 1 | 0.1 | 1 | 1 |
| 9 - Segment 9. | 2 | 0.1 | 1 | 0.1 | 0 | 0 | 0 | 1 |
| 10 - Segment 10. | 6 | 0.6 | 5 | 0.5 | 1 | 0.1 | 0 | 0 |
| **Totals** | **332** | **7** | **195** | **5.573** | **65** | **1.427** | **34** | **38** |

### Individual Ballot Pool Results

| Segment | Organization | Member | Ballot | Comments |
|---|---|---|---|---|
| 1 | Ameren Services | Kirit Shah | Negative | View |
| 1 | American Electric Power | Paul B. Johnson | Affirmative | View |
| 1 | American Transmission Company, LLC | Andrew Z Pusztai | Affirmative | |
| 1 | Arizona Public Service Co. | Robert Smith | Affirmative | |
| 1 | Associated Electric Cooperative, Inc. | John Bussman | Affirmative | |
| 1 | Avista Corp. | Scott J Kinney | Abstain | |
| 1 | Balancing Authority of Northern California | Kevin Smith | Affirmative | |
| 1 | Baltimore Gas & Electric Company | Gregory S Miller | Affirmative | View |

| | | | | |
|---|---|---|---|---|
| 1 | BC Hydro and Power Authority | Patricia Robertson | Abstain | |
| 1 | Beaches Energy Services | Joseph S Stonecipher | Affirmative | |
| 1 | Black Hills Corp | Eric Egge | Affirmative | |
| 1 | Bonneville Power Administration | Donald S. Watkins | Affirmative | View |
| 1 | Brazos Electric Power Cooperative, Inc. | Tony Kroskey | Negative | View |
| 1 | CenterPoint Energy Houston Electric, LLC | John Brockhan | Affirmative | |
| 1 | City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power | Chang G Choi | Affirmative | |
| 1 | Clark Public Utilities | Jack Stamper | Affirmative | |
| 1 | Colorado Springs Utilities | Paul Morland | Abstain | |
| 1 | Consolidated Edison Co. of New York | Christopher L de Graffenried | Affirmative | View |
| 1 | Corporate Risk Solutions, Inc. | Joseph Doetzl | Negative | |
| 1 | CPS Energy | Richard Castrejana | Affirmative | |
| 1 | Dominion Virginia Power | Michael S Crowley | Negative | |
| 1 | Duke Energy Carolina | Douglas E. Hils | Affirmative | |
| 1 | Entergy Services, Inc. | Edward J Davis | Negative | |
| 1 | FirstEnergy Corp. | William J Smith | Negative | View |
| 1 | Florida Keys Electric Cooperative Assoc. | Dennis Minton | Affirmative | |
| 1 | Florida Power & Light Co. | Mike O'Neil | Negative | |
| 1 | FortisBC | Curtis Klashinsky | Affirmative | |
| 1 | Georgia Transmission Corporation | Jason Snodgrass | Affirmative | |
| 1 | Great River Energy | Gordon Pietsch | Negative | View |
| 1 | Hoosier Energy Rural Electric Cooperative, Inc. | Bob Solomon | Negative | |
| 1 | Hydro One Networks, Inc. | Ajay Garg | Affirmative | |
| 1 | Idaho Power Company | Ronald D. Schellberg | Affirmative | |
| 1 | Imperial Irrigation District | Tino Zaragoza | Affirmative | View |
| 1 | International Transmission Company Holdings Corp | Michael Moltane | Affirmative | |
| 1 | Kansas City Power & Light Co. | Michael Gammon | Affirmative | |
| 1 | Lakeland Electric | Larry E Watt | Affirmative | |
| 1 | Lincoln Electric System | Doug Bantam | Affirmative | |
| 1 | Long Island Power Authority | Robert Ganley | | |
| 1 | Los Angeles Department of Water & Power | John Burnett | | |
| 1 | Lower Colorado River Authority | Martyn Turner | | |
| 1 | Manitoba Hydro | Joe D Petaski | Affirmative | |
| 1 | MEAG Power | Danny Dees | Affirmative | |
| 1 | MidAmerican Energy Co. | Terry Harbour | Negative | View |
| 1 | Minnesota Power, Inc. | Randi K. Nyholm | Affirmative | |
| 1 | Minnkota Power Coop. Inc. | Theresa Allard | Affirmative | |
| 1 | Nebraska Public Power District | Cole C Brodine | Affirmative | |
| 1 | New York Power Authority | Bruce Metruck | Affirmative | |
| 1 | Northeast Utilities | David Boguslawski | Affirmative | |
| 1 | Northern Indiana Public Service Co. | Kevin M Largura | Affirmative | |
| 1 | NorthWestern Energy | John Canavan | Abstain | |
| 1 | Ohio Valley Electric Corp. | Robert Mattey | Affirmative | |
| 1 | Oklahoma Gas and Electric Co. | Marvin E VanBebber | Abstain | |
| 1 | Omaha Public Power District | Doug Peterchuck | Negative | View |
| 1 | Oncor Electric Delivery | Jen Fiegel | | |
| 1 | PacifiCorp | Ryan Millard | Affirmative | |
| 1 | PECO Energy | Ronald Schloendorn | Abstain | |
| 1 | Platte River Power Authority | John C. Collins | Affirmative | |
| 1 | Portland General Electric Co. | John T Walker | Abstain | |
| 1 | Potomac Electric Power Co. | David Thorne | Affirmative | |
| 1 | PowerSouth Energy Cooperative | Larry D Avery | Affirmative | |
| 1 | PPL Electric Utilities Corp. | Brenda L Truhe | Affirmative | |
| 1 | Progress Energy Carolinas | Brett A Koelsch | Negative | View |
| 1 | Public Service Company of New Mexico | Laurie Williams | Affirmative | |
| 1 | Public Service Electric and Gas Co. | Kenneth D. Brown | Affirmative | |
| 1 | Puget Sound Energy, Inc. | Denise M Lietz | Abstain | |
| 1 | Rochester Gas and Electric Corp. | John C. Allen | Affirmative | |
| 1 | Sacramento Municipal Utility District | Tim Kelley | Affirmative | |
| 1 | Salt River Project | Robert Kondziolka | Negative | View |
| 1 | SCE&G | Henry Delk, Jr. | | |
| 1 | Seattle City Light | Pawel Krupa | Abstain | |
| 1 | Sierra Pacific Power Co. | Rich Salgo | Affirmative | |
| 1 | Snohomish County PUD No. 1 | Long T Duong | Affirmative | |
| 1 | South California Edison Company | Steven Mavis | Affirmative | |

| | | | | |
|---|---|---|---|---|
| 1 | Southern Company Services, Inc. | Robert A. Schaffeld | Negative | View |
| 1 | Southwest Transmission Cooperative, Inc. | James Jones | Negative | View |
| 1 | Sunflower Electric Power Corporation | Noman Lee Williams | Affirmative | |
| 1 | Tampa Electric Co. | Beth Young | Negative | |
| 1 | Tennessee Valley Authority | Larry Akens | | |
| 1 | Trans Bay Cable LLC | Steven Powell | Abstain | |
| 1 | Tri-State G & T Association, Inc. | Tracy Sliman | Affirmative | |
| 1 | Tucson Electric Power Co. | John Tolo | Affirmative | |
| 1 | United Illuminating Co. | Jonathan Appelbaum | Negative | |
| 1 | Westar Energy | Allen Klassen | Affirmative | |
| 1 | Western Area Power Administration | Brandy A Dunn | Affirmative | |
| 1 | Xcel Energy, Inc. | Gregory L Pieper | | |
| 2 | Alberta Electric System Operator | Mark B Thompson | Abstain | View |
| 2 | BC Hydro | Venkataramakrishnan Vinnakota | Abstain | |
| 2 | California ISO | Rich Vine | Affirmative | View |
| 2 | Electric Reliability Council of Texas, Inc. | Charles B Manning | Affirmative | View |
| 2 | Independent Electricity System Operator | Barbara Constantinescu | Affirmative | |
| 2 | ISO New England, Inc. | Kathleen Goodman | Affirmative | |
| 2 | Midwest ISO, Inc. | Marie Knox | Affirmative | View |
| 2 | New Brunswick System Operator | Alden Briggs | Affirmative | |
| 2 | New York Independent System Operator | Gregory Campoli | Affirmative | |
| 2 | Southwest Power Pool, Inc. | Charles H. Yeung | | |
| 3 | AEP | Michael E Deloach | Affirmative | View |
| 3 | Alabama Power Company | Richard J. Mandes | Negative | View |
| 3 | Ameren Services | Mark Peters | Negative | |
| 3 | APS | Steven Norris | Affirmative | |
| 3 | Arkansas Electric Cooperative Corporation | Philip Huff | Affirmative | |
| 3 | Atlantic City Electric Company | NICOLE BUCKMAN | Affirmative | |
| 3 | BC Hydro and Power Authority | Pat G. Harrington | Abstain | |
| 3 | Bonneville Power Administration | Rebecca Berdahl | Affirmative | |
| 3 | Central Lincoln PUD | Steve Alexanderson | Negative | View |
| 3 | City of Austin dba Austin Energy | Andrew Gallo | Affirmative | |
| 3 | City of Clewiston | Lynne Mila | Affirmative | |
| 3 | City of Farmington | Linda R Jacobson | Affirmative | |
| 3 | City of Garland | Ronnie C Hoeinghaus | Negative | View |
| 3 | City of Green Cove Springs | Gregg R Griffin | Affirmative | |
| 3 | City of Redding | Bill Hughes | Affirmative | |
| 3 | Consolidated Edison Co. of New York | Peter T Yost | Affirmative | |
| 3 | Constellation Energy | CJ Ingersoll | Affirmative | |
| 3 | Consumers Energy | Richard Blumenstock | Abstain | |
| 3 | Cowlitz County PUD | Russell A Noble | Affirmative | View |
| 3 | CPS Energy | Jose Escamilla | Affirmative | |
| 3 | Dayton Power & Light Co. | Jeffrey Fuller | Affirmative | |
| 3 | Delmarva Power & Light Co. | Michael R. Mayer | Affirmative | |
| 3 | Detroit Edison Company | Kent Kujala | Affirmative | |
| 3 | Dominion Resources Services | Michael F. Gildea | Negative | |
| 3 | Duke Energy Carolina | Henry Ernst-Jr | Affirmative | |
| 3 | Entergy | Joel T Plessinger | Negative | |
| 3 | FirstEnergy Energy Delivery | Stephan Kern | Negative | View |
| 3 | Flathead Electric Cooperative | John M Goroski | Affirmative | |
| 3 | Florida Municipal Power Agency | Joe McKinney | Affirmative | |
| 3 | Florida Power Corporation | Lee Schuster | Negative | View |
| 3 | Georgia Power Company | Danny Lindsey | Negative | View |
| 3 | Georgia Systems Operations Corporation | William N. Phinney | Affirmative | |
| 3 | Great River Energy | Brian Glover | Negative | View |
| 3 | Gulf Power Company | Paul C Caldwell | Negative | View |
| 3 | Hydro One Networks, Inc. | David Kiguel | Affirmative | |
| 3 | Imperial Irrigation District | Jesus S. Alcaraz | Affirmative | |
| 3 | JEA | Garry Baker | Affirmative | |
| 3 | Kansas City Power & Light Co. | Charles Locke | Affirmative | |
| 3 | Kissimmee Utility Authority | Gregory D Woessner | | |
| 3 | Lakeland Electric | Norman D Harryhill | Affirmative | |
| 3 | Lincoln Electric System | Jason Fortik | Affirmative | |
| 3 | Los Angeles Department of Water & Power | Daniel D Kurowski | | |
| 3 | Louisville Gas and Electric Co. | Charles A. Freibert | Affirmative | |
| 3 | Manitoba Hydro | Greg C. Parent | Affirmative | |

| | | | | |
|---|---|---|---|---|
| 3 | MidAmerican Energy Co. | Thomas C. Mielnik | Negative | |
| 3 | Mississippi Power | Jeff Franklin | Negative | View |
| 3 | Municipal Electric Authority of Georgia | Steven M. Jackson | Affirmative | |
| 3 | Nebraska Public Power District | Tony Eddleman | Affirmative | |
| 3 | New York Power Authority | David R Rivera | Affirmative | |
| 3 | Niagara Mohawk (National Grid Company) | Michael Schiavone | Affirmative | |
| 3 | Northern Indiana Public Service Co. | William SeDoris | Affirmative | |
| 3 | Omaha Public Power District | Blaine R. Dinwiddie | Negative | View |
| 3 | Orange and Rockland Utilities, Inc. | David Burke | Affirmative | |
| 3 | Orlando Utilities Commission | Ballard K Mutters | Affirmative | |
| 3 | Owensboro Municipal Utilities | Thomas T Lyons | Affirmative | |
| 3 | Pacific Gas and Electric Company | John H Hagen | Negative | View |
| 3 | PacifiCorp | Dan Zollner | Affirmative | |
| 3 | Platte River Power Authority | Terry L Baker | Affirmative | |
| 3 | PNM Resources | Michael Mertz | Affirmative | |
| 3 | Potomac Electric Power Co. | Robert Reuter | | |
| 3 | Progress Energy Carolinas | Sam Waters | | |
| 3 | Public Service Electric and Gas Co. | Jeffrey Mueller | Affirmative | |
| 3 | Public Utility District No. 1 of Benton County | Gloria Bender | Affirmative | |
| 3 | Public Utility District No. 1 of Clallam County | David Proebstel | Affirmative | |
| 3 | Puget Sound Energy, Inc. | Erin Apperson | | |
| 3 | Sacramento Municipal Utility District | James Leigh-Kendall | Affirmative | |
| 3 | Salt River Project | John T. Underhill | Negative | View |
| 3 | San Diego Gas & Electric | Scott Peterson | | |
| 3 | Seattle City Light | Dana Wheelock | Abstain | |
| 3 | Seminole Electric Cooperative, Inc. | James R Frauen | Affirmative | |
| 3 | Snohomish County PUD No. 1 | Mark Oens | Affirmative | |
| 3 | South Carolina Electric & Gas Co. | Hubert C Young | | |
| 3 | Tampa Electric Co. | Ronald L Donahey | Negative | |
| 3 | Tennessee Valley Authority | Ian S Grant | | |
| 3 | Tri-State G & T Association, Inc. | Janelle Marriott | Affirmative | |
| 3 | Westar Energy | Bo Jones | Affirmative | |
| 3 | Wisconsin Electric Power Marketing | James R Keller | Affirmative | |
| 3 | Xcel Energy, Inc. | Michael Ibold | Affirmative | |
| 4 | American Municipal Power | Kevin Koloini | Negative | |
| 4 | Blue Ridge Power Agency | Duane S Dahlquist | Abstain | |
| 4 | City of Austin dba Austin Energy | Reza Ebrahimian | Affirmative | |
| 4 | City of Clewiston | Kevin McCarthy | Affirmative | |
| 4 | City of Redding | Nicholas Zettel | Affirmative | |
| 4 | City Utilities of Springfield, Missouri | John Allen | Abstain | |
| 4 | Consumers Energy | David Frank Ronk | Affirmative | |
| 4 | Cowlitz County PUD | Rick Syring | Affirmative | |
| 4 | Flathead Electric Cooperative | Russ Schneider | Affirmative | |
| 4 | Florida Municipal Power Agency | Frank Gaffney | Affirmative | |
| 4 | Fort Pierce Utilities Authority | Thomas Richards | | |
| 4 | Georgia System Operations Corporation | Guy Andrews | Affirmative | |
| 4 | Madison Gas and Electric Co. | Joseph DePoorter | Affirmative | View |
| 4 | Northern California Power Agency | Tracy R Bibb | | |
| 4 | Ohio Edison Company | Douglas Hohlbaugh | Negative | View |
| 4 | Old Dominion Electric Coop. | Mark Ringhausen | Affirmative | |
| 4 | Public Utility District No. 1 of Douglas County | Henry E. LuBean | Affirmative | |
| 4 | Public Utility District No. 1 of Snohomish County | John D Martinsen | Affirmative | |
| 4 | Sacramento Municipal Utility District | Mike Ramirez | Affirmative | |
| 4 | Seattle City Light | Hao Li | Abstain | |
| 4 | Seminole Electric Cooperative, Inc. | Steven R Wallace | Affirmative | |
| 4 | Tacoma Public Utilities | Keith Morisette | | |
| 4 | Wisconsin Energy Corp. | Anthony Jankowski | Affirmative | View |
| 5 | AEP Service Corp. | Brock Ondayko | Affirmative | View |
| 5 | Amerenue | Sam Dwyer | Negative | |
| 5 | Arizona Public Service Co. | Edward Cambridge | Affirmative | |
| 5 | Avista Corp. | Edward F. Groce | Abstain | |
| 5 | BC Hydro and Power Authority | Clement Ma | Abstain | |
| 5 | Bonneville Power Administration | Francis J. Halpin | Affirmative | View |
| 5 | Brazos Electric Power Cooperative, Inc. | Shari Heino | Negative | View |
| 5 | City and County of San Francisco | Daniel Mason | Negative | View |
| 5 | City of Austin dba Austin Energy | Jeanie Doty | Affirmative | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 5 | City of Redding | Paul Cummings | Affirmative | |
| 5 | City Water, Light & Power of Springfield | Steve Rose | | |
| 5 | Cleco Power | Stephanie Huffman | | |
| 5 | Colorado Springs Utilities | Jennifer Eckels | Affirmative | |
| 5 | Consolidated Edison Co. of New York | Wilket (Jack) Ng | Affirmative | |
| 5 | Constellation Power Source Generation, Inc. | Amir Y Hammad | | |
| 5 | Consumers Energy Company | David C Greyerbiehl | Abstain | |
| 5 | Cowlitz County PUD | Bob Essex | Affirmative | |
| 5 | Dairyland Power Coop. | Tommy Drea | Affirmative | |
| 5 | Detroit Edison Company | Christy Wicke | Affirmative | |
| 5 | Dominion Resources, Inc. | Mike Garton | Negative | View |
| 5 | Duke Energy | Dale Q Goodwine | Affirmative | |
| 5 | Edison Mission Marketing & Trading Inc. | Brenda J Frazer | Affirmative | |
| 5 | Electric Power Supply Association | John R Cashin | Abstain | |
| 5 | Energy Services, Inc. | Tracey Stubbs | Negative | View |
| 5 | Essential Power, LLC | Patrick Brown | Negative | View |
| 5 | Exelon Nuclear | Michael Korchynsky | Abstain | |
| 5 | FirstEnergy Solutions | Kenneth Dresner | Negative | View |
| 5 | Florida Municipal Power Agency | David Schumann | Affirmative | |
| 5 | Great River Energy | Preston L Walsh | | |
| 5 | Imperial Irrigation District | Marcela Y Caballero | Affirmative | |
| 5 | JEA | John J Babik | Affirmative | |
| 5 | Kansas City Power & Light Co. | Brett Holland | Affirmative | |
| 5 | Kissimmee Utility Authority | Mike Blough | Affirmative | |
| 5 | Lakeland Electric | James M Howard | | |
| 5 | Liberty Electric Power LLC | Daniel Duff | Negative | |
| 5 | Lincoln Electric System | Dennis Florom | Affirmative | |
| 5 | Los Angeles Department of Water & Power | Kenneth Silver | | |
| 5 | Manitoba Hydro | S N Fernando | Affirmative | |
| 5 | Massachusetts Municipal Wholesale Electric Company | David Gordon | Abstain | |
| 5 | MEAG Power | Steven Grego | Affirmative | |
| 5 | MidAmerican Energy Co. | Christopher Schneider | Negative | |
| 5 | Muscatine Power & Water | Mike Avesing | Abstain | |
| 5 | Nebraska Public Power District | Don Schmit | Affirmative | |
| 5 | New York Power Authority | Wayne Sipperly | Affirmative | |
| 5 | NextEra Energy | Allen D Schriver | Negative | |
| 5 | Northern Indiana Public Service Co. | William O. Thompson | Affirmative | |
| 5 | Occidental Chemical | Michelle R DAntuono | Negative | View |
| 5 | Omaha Public Power District | Mahmood Z. Safi | Negative | View |
| 5 | PacifiCorp | Sandra L. Shaffer | Affirmative | |
| 5 | Platte River Power Authority | Roland Thiel | Affirmative | |
| 5 | Portland General Electric Co. | Gary L Tingley | | |
| 5 | PPL Generation LLC | Annette M Bannon | Affirmative | |
| 5 | Progress Energy Carolinas | Wayne Lewis | Negative | View |
| 5 | PSEG Fossil LLC | Tim Kucey | Affirmative | |
| 5 | Public Utility District No. 1 of Douglas County | Curtis A Wilkins | Affirmative | |
| 5 | Public Utility District No. 1 of Lewis County | Steven Grega | Abstain | |
| 5 | Puget Sound Energy, Inc. | Tom Flynn | | |
| 5 | Sacramento Municipal Utility District | Bethany Hunter | Affirmative | |
| 5 | Salt River Project | William Alkema | Negative | View |
| 5 | Seattle City Light | Michael J. Haynes | Abstain | |
| 5 | Seminole Electric Cooperative, Inc. | Brenda K. Atkins | | |
| 5 | Snohomish County PUD No. 1 | Sam Nietfeld | Affirmative | |
| 5 | South Carolina Electric & Gas Co. | Edward Magic | | |
| 5 | Southern California Edison Co. | Denise Yaffe | Affirmative | |
| 5 | Southern Company Generation | William D Shultz | Negative | View |
| 5 | Tacoma Power | Claire Lloyd | Affirmative | View |
| 5 | Tampa Electric Co. | RJames Rocha | Negative | |
| 5 | Tenaska, Inc. | Scott M. Helyer | Abstain | |
| 5 | Tennessee Valley Authority | David Thompson | | |
| 5 | Tri-State G & T Association, Inc. | Barry Ingold | | |
| 5 | U.S. Army Corps of Engineers | Melissa Kurtz | Negative | View |
| 5 | U.S. Bureau of Reclamation | Martin Bauer | Affirmative | |
| 5 | Westar Energy | Bryan Taggart | Affirmative | |
| 5 | Wisconsin Electric Power Co. | Linda Horn | Affirmative | |
| 6 | AEP Marketing | Edward P. Cox | Affirmative | View |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 6 | Ameren Energy Marketing Co. | Jennifer Richardson | Negative | |
| 6 | APS | RANDY A YOUNG | Affirmative | |
| 6 | Bonneville Power Administration | Brenda S. Anderson | Affirmative | |
| 6 | City of Austin dba Austin Energy | Lisa L Martin | Affirmative | |
| 6 | City of Redding | Marvin Briggs | Affirmative | |
| 6 | Cleco Power LLC | Robert Hirchak | | |
| 6 | Consolidated Edison Co. of New York | Nickesha P Carrol | Affirmative | |
| 6 | Constellation Energy Commodities Group | Brenda L Powell | Affirmative | |
| 6 | Entergy Services, Inc. | Terri F Benoit | Negative | |
| 6 | Exelon Power Team | Pulin Shah | Abstain | |
| 6 | FirstEnergy Solutions | Kevin Querry | Negative | View |
| 6 | Florida Municipal Power Agency | Richard L. Montgomery | Affirmative | |
| 6 | Florida Municipal Power Pool | Thomas Washburn | Affirmative | |
| 6 | Florida Power & Light Co. | Silvia P. Mitchell | Negative | |
| 6 | Great River Energy | Donna Stephenson | | |
| 6 | Imperial Irrigation District | Cathy Bretz | Affirmative | |
| 6 | Kansas City Power & Light Co. | Jessica L Klinghoffer | Affirmative | |
| 6 | Lakeland Electric | Paul Shipps | Affirmative | |
| 6 | Lincoln Electric System | Eric Ruskamp | Affirmative | |
| 6 | Los Angeles Department of Water & Power | Brad Packer | | |
| 6 | Luminant Energy | Brad Jones | Abstain | |
| 6 | Manitoba Hydro | Daniel Prowse | Affirmative | View |
| 6 | MidAmerican Energy Co. | Dennis Kimm | Negative | |
| 6 | New York Power Authority | Saul Rojas | Affirmative | |
| 6 | Northern Indiana Public Service Co. | Joseph O'Brien | Affirmative | View |
| 6 | NRG Energy, Inc. | Alan Johnson | Abstain | |
| 6 | Omaha Public Power District | David Ried | Negative | View |
| 6 | PacifiCorp | Scott L Smith | Affirmative | |
| 6 | Platte River Power Authority | Carol Ballantine | Affirmative | |
| 6 | Powerex Corp. | Daniel W. O'Hearn | | |
| 6 | PPL EnergyPlus LLC | Mark A Heimbach | Affirmative | |
| 6 | Progress Energy | John T Sturgeon | Negative | View |
| 6 | PSEG Energy Resources & Trade LLC | Peter Dolan | Affirmative | |
| 6 | Public Utility District No. 1 of Chelan County | Hugh A. Owen | Abstain | |
| 6 | Sacramento Municipal Utility District | Diane Enderby | Affirmative | |
| 6 | Salt River Project | Steven J Hulet | Negative | View |
| 6 | Seattle City Light | Dennis Sismaet | Abstain | |
| 6 | Seminole Electric Cooperative, Inc. | Trudy S. Novak | Affirmative | |
| 6 | Snohomish County PUD No. 1 | William T Moojen | Affirmative | |
| 6 | South California Edison Company | Lujuanna Medina | Affirmative | |
| 6 | Southern Company Generation and Energy Marketing | John J. Ciza | Negative | View |
| 6 | Tacoma Public Utilities | Michael C Hill | Affirmative | |
| 6 | Tampa Electric Co. | Benjamin F Smith II | Negative | |
| 6 | Tennessee Valley Authority | Marjorie S. Parsons | | |
| 6 | Westar Energy | Grant L Wilkerson | Affirmative | |
| 8 | | Edward C Stein | | |
| 8 | | Roger C Zaklukiewicz | Affirmative | |
| 8 | | James A Maenner | Abstain | |
| 8 | APX | Michael Johnson | Affirmative | |
| 8 | JDRJC Associates | Jim Cyrulewski | Affirmative | |
| 8 | Massachusetts Attorney General | Frederick R Plett | Affirmative | |
| 8 | Network & Security Technologies | Nicholas Lauriat | Affirmative | |
| 8 | Volkmann Consulting, Inc. | Terry Volkmann | Negative | |
| 9 | California Energy Commission | William M Chamberlain | | |
| 9 | Commonwealth of Massachusetts Department of Public Utilities | Donald Nelson | Affirmative | |
| 10 | New York State Reliability Council | Alan Adamson | Affirmative | |
| 10 | Northeast Power Coordinating Council | Guy V. Zito | Affirmative | |
| 10 | ReliabilityFirst Corporation | Anthony E Jablonski | Affirmative | |
| 10 | Southwest Power Pool RE | Emily Pennel | Negative | View |
| 10 | Texas Reliability Entity, Inc. | Donald G Jones | Affirmative | |
| 10 | Western Electricity Coordinating Council | Steven L. Rueckert | Affirmative | |
| | | | | |

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
*Washington Office:* 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

**Individual or group. (39 Responses)**
**Name (25 Responses)**
**Organization (25 Responses)**
**Group Name (14 Responses)**
**Lead Contact (14 Responses)**
**Question 1 (38 Responses)**
**Question 1 Comments (39 Responses)**
**Question 2 (37 Responses)**
**Question 2 Comments (39 Responses)**
**Question 3 (37 Responses)**
**Question 3 Comments (39 Responses)**

| |
|---|
| |
| Individual |
| Keira Kazmerski |
| Xcel Energy |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Individual |
| Jay Walker |
| NIPSCO |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Group |
| PacifiCorp |
| Sandra Shaffer |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Group |
| Southern Company |
| Shane Eaker |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation expands the reach of the standard. |
| |
| No |
| Comments: Question 2 and 3 from the Request for Interpretation are not answered by the interpretation. The answers simply describe how the CIP standards do not address the questions being asked. The standards do not address the scenario contemplated by the line of questioning and |

| |
|---|
| should be remanded to the CIP SDT to fix in version 5 of the standards. Comment: Vendor support personnel dispatched to the various generation sites are selected base upon their physical availability and the expertise required on the projects. It is a difficult task to provide ongoing training and background checks for every potential individual from numerous vendors supporting a variety of systems. It is near impossible to monitor the ongoing employment status of this large number of vendor personnel, to assure timely removal from the access control list, that will be required if implemented as discussed in the proposed interpretation. At present, vendor personnel supplying setup/support may work freely on pre-shipped non-installed systems. This trusted relationship should be extended, to similar individuals under escort at the equipment site. If the support function requires that changes be made to systems, having site personnel follow the direction of the vendor expert presents an increase potential for error, while adding marginal security benefits. |
| Individual |
| Ronnie Hoeinghaus |
| City of Garland |
| The request is asking for clarity on the application of a requirement. |
| |
| |
| No |
| Disagree with the concept of there being no escorted Cyber Access. If someone with authorized access is working with a vendor or contractor on an issue, the system is more secure than if you give him authorized access just because he has a PRA and has had CIP training. Take for example, Hector Xavier Monsegur, the notorious hacker known as Sabu and leader of LulzSec. Because of his cooperation and work with the FBI and other agencies, he may end up with his record cleansed or at least be able to put on a resume his work with the FBI. Eight years from now, a 7 year criminal background check could be clear. If a company were to utilize him for a short term issue, would the company be more secure with him being “escorted” or with him being issued authorized access and allowed free access. It is noted in your supporting comments that the standard requirements do not state specifically that escorted cyber access is permitted. On the other hand, the standard requirements do not have statements preventing escorted cyber access either. Which is more secure? |
| Individual |
| Andrew Z. Pusztai |
| American Transmission Company, LLC |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Group |
| Northeast Power Coordinating Council |
| Guy Zito |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Individual |
| Thad Ness |
| American Electric Power |
| The request is asking for clarity on the meaning of a requirement. |
| |

| |
|---|
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| AEP agrees with the overall interpretation, but offers the following commentsand recommendations for improving the interpretation. Responses to Questions 1 and 2: The response provided for Q1 does not definitively answer the question that was posed. The question posed asks what the definition is for “authorized access”, while the response essentially states that one has this access by being on the proper list. It is not clear from the response how those on the authorized list were added to it, i.e. that those individuals met the necessary training, risk assessment, and access requirements. This might be made clearer if, rather than generally mentioning R2, R3, and R4, specifically stating what those requirements are. The response provided for Question 2 more adequately addresses Question 1 than does the response to Q1. |
| Individual |
| Randi Nyholm |
| Minnesota Power |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Group |
| Southwest Power Pool Regional Entity |
| Emily Pennel |
| The request is asking for clarity on the application of a requirement. |
| The clarification requested by WECC specifically states that the WECC RC seeks clarification on the definition of authorized access "as applied to temporary support from vendors." |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| The SPP RE agrees with the interpretation, noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent the escorted individual from overtly, covertly, or inadvertently causing harm. Granting direct cyber access to someone without authorized access inhibits the ability to perform the escort responsibilities and introduces risk. As noted in the interpretation, this is why the standard specifically makes a distinction regarding "authorized, unescorted" physical access. Technically, escorted cyber access is not feasible. The SPP RE agrees that "over the shoulder" viewing via a webinar or close proximity presence, while possibly subject to the entity’s CIP-003/R5 information protection program, does not constitute cyber access. |
| Individual |
| Greg Rowland |
| Duke Energy |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Individual |
| Brian J Murphy |
| NextEra Energy Inc. |
| The request is asking for clarity on the application of a requirement. |

| |
|---|
| Each of the three questions is asking whether a class of individuals (i.e., temporary vendors and supervisors of vendors) is required to comply with CIP-004 R2, R3 and R4. Thus, the questions are requesting specific confirmation whether one is or is out of compliance based on how these classes of individuals are addressed under CIP-004. |
| The interpretation expands the reach of the standard. |
| It could be viewed that the interpretation requested tends to expand the reach of CIP-004, given the lack of clarity in the answers. Thus, if this interpretation goes forward, it is recommended that that the following clearer and more to the point answers be substituted for the current answers, so there is no expanding of CIP-004 nor an elaboration on how the standard applies to particular facts: 1. WECC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors. Answer: The term authorized access as used in CIP-004 is not limited or qualified by any type or class of employees or vendors. Thus, all employees and vendors (who desire either physical or cyber access) without regard to whether they are temporary support or not must either: (1) be escorted by someone with authorized unescorted physical or authorized cyber access, as applicable or (2) have been granted authorized unescorted physical or authorized cyber access by meeting the requirements of R2 and R3. Thus, there is no exception for temporary support from vendors, and the term authorized access applies to them in the same manner it applies to any other class or type of employee or vendor. 2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Answer: Yes. The language of CIP-004 applies to all employees and vendors that desire unescorted physical or cyber access to Critical Cyber Assets without regard to whether or not the employee or vendor is supervised. 3. Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? Answer. See answer to question 2 – supervised vendors are not exempt from CIP-004-1, Requirements R2, R3, and R4, thus the remainder of the question is moot. |
| No |
| As written, this interpretation should either be dismissed as in appropriate or the answers re-written to be clearer and more responsive. See answers to question 1 and 2. |
| Group |
| Bonneville Power Administration |
| Chris Higgins |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| BPA believes that if the drafting team allowed for the concept of supervised cyber access, they would be expanding the scope CIP-004. |
| Yes |
| |
| Individual |
| Michelle R D'Antuono |
| Ingleside Cogeneration LP |
| The request is asking for clarity on the meaning of a requirement. |
| WECC has requested a clarification of the definition of “authorized access” to determine if vendor personnel who provide supervised temporary support to Responsible Entities, are subject to CIP-004 R2 through R4. This is a subject of great relevance to Ingleside Cogeneration LP as we require all of our vendors to maintain robust cyber security programs, but agree with WECC that a literal reading of CIP-004 may require dedicated agents from each. Critical vendors such as Cisco or GE do not support an operating model like this – and we would argue that their security training and personnel screening procedures are superior. This subject will become especially prevalent when CIP Version 5 takes effect and all Responsible Entities will be required to have a cyber policy that addresses Cyber System Access. We would like to see this complex issue addressed now, before some precedence is set that proves to be uneconomical or unviable. |
| The interpretation expands the reach of the standard. |

| |
|---|
| The project team has chosen to differentiate between escorted physical access where a vendor performs a non-cyber activity (such as replacing parts) from one where a cyber connection has been made. Ingleside Cogeneration LP believes the project team has read in extra language into the requirement – and changed FERC's intent in Order 706 paragraph 432. That paragraph was cited by WECC in the original Request for Interpretation, and clearly acknowledges that supervised access is a real-life operational need under certain circumstances. If anything, the Commission brings up a good point about the qualifications of the escort, but it does not seem appropriate that the drafting team has completely ruled out supervised cyber access. Furthermore, by logical inference, if the Responsible Entity can demonstrate that they can supervise remote cyber access, then that should be allowed as well. |
| No |
| Ingleside Cogeneration LP believes that the interpretation is an overly-literal reading of CIP-004 and may hamper routine technical support processes with no demonstrable reduction in cyber-risk . The power and convenience of remote vendor maintenance may be unavailable to all but the largest utilities should costs rise because of it. Such a result will actually diminish BES reliability as access to highly competent technical support and maintenance personnel becomes restricted. There may be acceptable solutions, however. It would seem that a single cyber certification of vendors such as Cisco and GE could be referenced in thousands of individual security policies. Alternatively, the industry could provide a single generic cyber training package and employee background check method for vendors. We would hope that NERC takes a leadership position in resolving these complex issues. Lastly, the industry needs more direction than that provided in the circular response to the first question. The project team essentially states that the Responsible Entity must determine who has authorized access to their Critical Cyber Assets and include them on an access list. That list will then define authorized access – leaving the door open for a wide variety of resolutions. |
| Individual |
| . |
| . |
| |
| |
| |
| Individual |
| Michael Falvo |
| Independent Electricity System Operator |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Individual |
| Kim Koster |
| MidAmerican Energy Company |
| The request is asking for clarity on the application of a requirement. |
| The request is asking for clarification on the application of the term "authorized access" in order to determine how to comply in the situation of temporary vendor support. |
| The interpretation expands the reach of the standard. |
| WECC is seeking "clarification on the definition of 'authorized access.'" |
| No |
| The request is asking how to comply with one or more requirements in a specific situation with vendor support. Requests as to how to comply, per the Rules of Procedure, do not meet the valid criteria of an interpretation request. While we agree with the conclusion in the proposed response, the draft response restates information that already is in the standard. |

| |
|---|
| Group |
| Dominion |
| Connie Lowe |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation expands the reach of the standard. |
| The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard. |
| No |
| The following Dominion responses are provided in order of the questions asked by WECC: 1. The interpretation that individuals on the list of personnel authorized for cyber or unescorted physical access to CCAs are subject to CIP-004-1 R2, R3 (with allowed restrictions), and R4 is appropriate. 2. CIP-004-1-R4 specifically addresses authorized access and does not state that “all cyber access to Critical Cyber Assets must be authorized”. CIP-004-1-R2 and CIP-004-1-R3 (with allowed restrictions) apply to "personnel having authorized cyber or authorized unescorted physical access". The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard. 3. The concept of "escorted electronic access" is absent from CIP-004-1. Absent a standard, it should be up to each Registered Entity to determine by internal policy whether or not escorted electronic access should be allowed. |
| Individual |
| Kirit Shah |
| Ameren |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation expands the reach of the standard. |
| |
| No |
| The CIP-004 R4 IDT interpretation relies on incorrect logic in stating that Standard does not allow for escorted (supervised) cyber access to cyber assets solely because "unescorted cyber" is not explicitly included in the CIP-004 R4 "list". We agree with the idea put forth in the Requirement that anyone with unfettered cyber access is a potential danger and in like manner, so would anyone with unescorted physical access. However, the reason the Requirement does not require those with escorted cyber access to be listed is not because such access is somehow not contemplated or not permitted but rather because, like escorted physical access, these individuals, and their actions, are well monitored and controlled and do not need the extra care and handling that ensues from being on "The List" for those free to take independent action. The mere fact that they do not need further "handling" does not mean in any way that they do not exist or that this in not permitted. We are concerned that IDT is using a classic argument from the negative to imply something is impermissible on that such use is not contemplated merely because it is absent from a list of threat types that need to be addressed. |
| Individual |
| Jonathan Appelbaum |
| United Illuminating Company |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation expands the reach of the standard. |
| |
| No |
| The Interpretation DT correctly states that CIP-004 R2 and R3 apply to individuals on a list |

| |
|---|
| designating them with authorized cyber access or authorized unescorted physical access to Critical Cyber Assets. The Interpretation DT makes an error in stating that CIP-004 limits the type of cyber access to a Critical Cyber Assets to only authorized individuals, that is, there is no opportunity to implement supervised remote access via terminal session (i.e. Webex) to support personnel not on the authorized cyber access list. The Reliability standards do not provide a definitive statement of the types of access allowed to Critical Cyber Assets. The Standards only provide the program requirements for three types of access; authorized physical, escorted physical, and authorized cyber. By not providing a definitive list of the types of access the original Drafting team did not exclude the type of access under review in this interpretation, that is, supervised cyber access via terminal session. At the time the Reliability standards was approved the concept of supervised remote access was known. The Interpretation Drafting Team can only conclude that the original Standard Drafting Team did not list specific requirements for this type of access. The Interpretation Drafting Team cannot conclude that this type of access was prohibited. The fact that CIP-007 does not contain a specific unescorted cyber access provision is irrelevant. CIP-007 R5 requires technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Supervised access via Webex is not unauthorized system access. When terminal session access is utilized, the activity is tracked by the Company. R5 does not state all authorized user activity, the Interpretation drafting team is adding the word authorized in its response and is expanding the scope. This conclusion is more sensible for service vendors and SCADA system providers. The Interpretation Drafting Team's interpretation would require, as the requestor noted, large vendors (such as CISCO) to take every entities cyber training course and submit to multiple background checks. This would be compliance for compliance sake and not for security. The Interpretation should have stated that the names of authorized individuals are maintained on a list. These individuals are required to comply with CIP-004 R2 through R4. Supervisory Cyber Access via terminal session is not prohibited explicitly by the Standards and is therefore allowed. There are no additional Reliability requirements for such access beyond those described in Standards CIP-002 through CIP-009. |
| Individual |
| Jim Eckelkamp |
| Progress Energy |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation expands the reach of the standard. |
| |
| No |
| Progress Energy disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or onsite cyber access). Registered Entities should be able to allow vendors providing support temporary, indirect, and monitored access to in scope NERC CIP assets via remote terminal sessions (Live Mtg, Webex, etc) (just as escorted physical access is allowed) without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. In addition, Registered Entities should be able to allow vendors providing onsite temporary support escorted cyber access without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. There are multiple NERC CIP support vendors that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard. This includes process control vendors not just IT vendors. Honeywell, GE, ABB, Siemens, Babcock and Wilcox, Emerson, GTE, Wood Group are all DCS vendors/tuners that may need to provide escorted cyber access at Progress Energy and throughout the industry. Not allowing for escorted cyber access could have adverse impacts to BES Reliability since some of this work is needed not only during emergencies but also for ongoing maintenance. Long term service agreements are in place with these vendors that have warranty implications that require escorted cyber support for various process control systems. Many Registered Entities rely on these vendors/tuners to provide their expertise in support of continual operations for proprietary systems and do not employ resources with these specialized skill sets. |
| Individual |

| |
|---|
| Andrew Ginter |
| Waterfall Security Solutions |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| No |
| Unidirectional remote screen view products using hardware-enforced unidirectional communications or "data diodes" can securely show remote, unauthorized personnel the contents of screens on Critical Cyber Assets which are inside of an ESP. The technology allows remote personnel to watch and advise as authorized individuals carry out cyber access to those CCAs without introducing any risk that the remote personnel can directly influence the monitored CCAs in any way. This mechanism addresses WECC's concern regarding being "excessively burdened by limiting access to timely support." Since unidirectional remote screen view technology prevents the unauthorized observer from carrying out any direct cyber access, the unidirectional technology should have been identified in the interpretation as a legitimate form of supervised remote access. |
| Individual |
| Thomas Johnson |
| Salt River Project |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| No |
| As written we disagree with the IDT team's interpretation of CIP-004. We recognize CIP-004 does not include the concept of any words relating to "escorting" or "supervision" in the requirement language. However, the interpretation is not clearly defined and reaches the conclusion that escorted electronic access is prohibited because a formal electronic access escorting requirement is not defined. It appears this conclusion was based on the fact that CIP-006 clearly defines "escorted" or "supervised" physical access to cyber assets. We believe this type of assumption sets a bad precedent for future interpretations. Additionally we believe this interpretation won't allow emergent electronic access when needed. We believe there is little or no risk associated with allowing escorted access to a known contracted support vendor, when support is needed. In fact we believe prohibiting this type of access increases the risk level to the BES. |
| Individual |
| Andrew Gallo |
| Austin Energy |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| No |
| We believe NERC should acknowledge that "escorted" cyber access is legitimate. If one of our employees is monitoring the cyber activities of the escorted vendor, our employee could terminate the session if the vendor began to take inappropriate actions. This is akin to the situation for escorted physical access. As long as the person is escorted, if s/he begins to take inappropriate action, the escort can take appropriate responsive action. |
| Group |
| Pepco Holdings Inc & Affiliates |
| David Thorne |
| The request is asking for clarity on the application of a requirement. |
| |

| |
|---|
| The interpretation does not expand the reach of the standard. |
| |
| No |
| It is understood why the SDT applied a strict interpretation which results in no change to the existing standard. The requested interpretation would have changed the meaning and reach of the standard. However there still remains a very serious real problem. There is a need to allow cyber access to a vendor on some sort of an emergency basis without meeting R2 and R3. The Impact Statement in the Request for Interpretation submitted by WECC is a very serious problem for many entities that could result in a high risk or serious system reliability problem. |
| Group |
| FirstEnergy |
| Sam Ciccone |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| No |
| There is an inherent flaw in the interpretation because it is based on an inactive standard CIP-004-1. The current effective standard is CIP-004-3 which differs in a significant way from CIP-004-1. Version 3 of this standard now allows exceptions in emergency situations as stated from the phrase “except in specified circumstances such as an emergency” which is included in R2.1 and R3. This specifically affects the answer to WECC’s third question. Remote and on-site cyber access should be allowed under supervision during emergency situations and it would be very difficult to assure that all personnel offering remote assistance in these situations were assessed per the requirements of CIP-004. A second inherent flaw is that the interpretation is based on an inactive standard CIP-006-1. The current effective standard CIP-006-3 expressly describes visitor supervision requirements. Per CIP-006-3, R1.6, visitors are required to be continuously escorted within Physical Security Perimeters. This revised requirement should be integrated into the answers to WECC’s second and third question. Therefore, we suggest the team revise the interpretation to only make reference to the current Version 3 standards, and add language in the interpretation that there are exceptions for emergency situations as specified by the entity per CIP-003 which requires details of those emergency situations. |
| Group |
| Tacoma Public Utilities |
| Kieth Morisette |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| Agree with the standard as written in the WECC position paper |
| Individual |
| Patrick Brown |
| Essential Power, LLC |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| No |
| In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation. In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory |

| |
|---|
| compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support. Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard. There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access. |
| Group |
| Kansas City Power & Light |
| Dean Larson |
| The request is asking for clarity on the application of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Individual |
| John Seelke |
| PSEG (Public Service Enterprise Group) |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| The inability to provide Escorted Cyber Access through a web-conference (or otherwise), can be detrimental to the reliability of the BES as the time to troubleshoot cyber/networking issues can be extensive without letting the remote support personnel have access to the troubled device. |
| Individual |
| Christina Bigelow |
| Midwest ISO |
| The request is asking for clarity on the meaning of a requirement. |
| The request seeks clarification of the meaning of "authorized access." As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof. |
| The interpretation expands the reach of the standard. |
| MISO respectfully submits that, based on a literal reading of the plain language of CIP-004, the phrase "authorized access" is not part of the language of the requirement requested for interpretation. The use of a specific term not utilized in the requirement as well as the assignment of a specific meaning and obligations from the requirement at issue to such a term by the Interpretation Drafting Team ("IDT") in its Interpretation expands the reach of the standard. |
| No |

MISO respectfully submits that the IDT's proposed Interpretation of the phrase “authorized access” is unsupported by the plain language of CIP-004. The phrase “authorized access,” which is the subject of the Interpretation, does not appear in CIP-004. Instead, the Standard uses the phrase “authorized cyber or authorized unescorted physical access.” MISO understands that the question posed by the requestor utilized the term “Authorized Access”, but respectfully submits that the IDT should have provided clarification specifically regarding authorized cyber access and authorized unescorted cyber access, which clarification would have resulted in entities ability to more directly apply the interpretation to its compliance efforts under CIP-004-1, R2. Moreover, the IDT’s explanation of “authorized access” merely refers back to the requirements associated with access without providing the requested clarification. As a result, MISO does not agree with the Interpretation as to the answer provided in response to Question 1. As to the proposed answers to Questions 2 and 3, MISO respectfully submits that, without the specific clarification requested under Question 1, the Interpretation’s conclusions are not sufficiently supported by the text of CIP-004.

Group

ISO/RTO Standards Review Committee

Gregory Campoli

The request is asking for clarity on the meaning of a requirement.

The interpretation does not expand the reach of the standard.

Yes

Individual

Ron Donahey

Tampa Electric Company

The request is asking for clarity on the meaning of a requirement.

The interpretation does not expand the reach of the standard.

Yes

Although we believe that the Interpretations Drafting Team has correctly provided the interpretation, we believe that the standard should be changed to provide a vehicle for emergency vendor access via cyber or physical escorting. The lack of the ability to provide this emergency access could be detrimental to the reliability of the grid and may force Entities into non-compliance to meet the emergency situation.

Group

ACES Power Marketing Collaborators

Jason Marshall

The request is asking for clarity on the meaning of a requirement.

The interpretation expands the reach of the standard.

Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines “authorized access’ by stating that an individual has “authorized access” if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated “authorized access” with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since Console access is almost

always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device.

No

This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus, maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. Three terms are defined or bounded outside the standards development process. These terms include: authorized access, cyber access and physical access. We will not repeat our arguments regarding this expansion of the standard here. They can be found in question 2. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary to the interpretation, most (probably all) registered entities have a formal process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed. We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert, software expert).

Group

MISO Standards Collaborators

Marie Knox

The request is asking for clarity on the application of a requirement.

| |
|---|
| The interpretation expands the reach of the standard. |
| |
| We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access. |
| Group |
| Imperial Irrigation District (IID) |
| Jesus Sammy Alcaraz |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| |
| Individual |
| Joe Doetzl |
| CRSI |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| No |
| The response to question 1 attempts to define authorized access. The definition, even if local to CIP-004, should be expanded to include an indication that authorized access indicates personnel with approval to access Critical Cyber Assets. The presence of a person's name on a maintained list could be in error and would not be an indication of authorized access. |
| Individual |
| Darryl Curtis |
| Oncor Electric Delivery Company |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |
| Oncor Electric Delivery agrees with this interpretation. The interpretation provides greater clarity on how a Compliance Enforcement Agency (CEA) addresses “cyber access” which includes both physical and remote acc |
| Individual |
| DANA SHOWALTER |
| E.ON CLIMATE & RENEWABLES |
| The request is asking for clarity on the meaning of a requirement. |
| |
| The interpretation does not expand the reach of the standard. |
| |
| Yes |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Consideration of Comments

## Interpretation of CIP-004-1 for Western Electricity Coordinating Council Project 2009-26

The Interpretation of CIP-004-1 for WECC Drafting Team thanks all commenters who submitted comments on the Interpretation of CIP-004-1 for the Western Electricity Coordinating Council (Project 2009-26). These standards were posted for a parallel 45-day public comment period and intial ballot from February 7, 2012 through March 23, 2012. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form. There were 38 sets of comments, including comments from approximately 99 different people from approximately 59 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page:

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

**Summary:**

The IDT carefully reviewed all comments in response to the posting for parallel formal comment period and ballot that ended March 23, 2012. In the draft interpretation the IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. While the IDT agrees with several commenters that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term in response to WECC's request for interpretation. After considering the comments, the IDT decided not to make any changes to its interpretation, and explains its rationale in response to several minority concerns below. The interpretation is being posted for a recirculation ballot.

- One commenter does not believe that the standard separates how to treat cyber and physical access for vendors with regard to supervision. Other commenters suggest 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, the IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. Furthermore, there are a number of contexts in which

someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).

- The IDT notes that the standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.
- Several commenters provided suggestions or comments that the drafting team was not able to address and stay within the Guidelines for Interpretation Drafting Teams, and the IDT recommends that commenters provide specific comments to address these issues when the Version 5 CIP standards are posted for comment.
- Several commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES. Furthermore, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams.
- Some commenters suggested that the absence of language regarding supervision or escorting with respect to electronic access does not absolutely prohibit the concept. In response, the IDT notes the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Commenters also suggest that the standards should be modified to allow for vendor or contractor access without having to satisfy the authorization requirements. However, modification of the standard is outside the scope of an interpretation. The IDT believes that the interpretation adequately addresses that all cyber access is contemplated by the interpretation, which includes both employees and vendors.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President of Standards and Training, Herb Schrayshuen, at 404-446-2560 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Reliability Standards Development Procedures: http://www.nerc.com/standards/newstandardsprocess.html.

## Index to Questions, Comments, and Responses

**The Industry Segments are:**

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1. | Group | Guy Zito | Northeast Power Coordinating Council | | | | | | | | | | X |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Alan Adamson | New York State Reliability Council, LLC | NPCC | 10 |
| 2. | Greg Campoli | New York Independent System Operator | NPCC | 2 |
| 3. | Sylvain Clermont | Hydro-Quebec TransEnergie | NPCC | 1 |
| 4. | Chris de Graffenried | Consolidated Edison Co. of New York, Inc. | NPCC | 1 |
| 5. | Gerry Dunbar | Northeast Power Coordinating Council | NPCC | 10 |
| 6. | Mike Garton | Dominion Resources Services, Inc. | NPCC | 5 |
| 7. | Kathleen Goodman | ISO - New England | NPCC | 2 |
| 8. | Chantel Haswell | FPL Group, Inc. | NPCC | 5 |
| 9. | David Kiguel | Hydro One Networks Inc. | NPCC | 1 |
| 10. | Michael R. Lombardi | Northeast Utilities | NPCC | 1 |

| Group/Individual | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

| | | | | |
|---|---|---|---|---|
| 11. | Randy MacDonald | New Brunswick Power Transmission | NPCC | 9 |
| 12. | Bruce Metruck | New York Power Authority | NPCC | 6 |
| 13. | Lee Pedowicz | Northeast Power Coordinating Council | NPCC | 10 |
| 14. | Robert Pellegrini | The United Illuminating Company | NPCC | 1 |
| 15. | Si-Truc Phan | Hydro-Quebec TransEnergie | NPCC | 1 |
| 16. | David Ramkalawan | Ontario Power Generation, Inc. | NPCC | 5 |
| 17. | Brian Robinson | Utility Services | NPCC | 8 |
| 18. | Saurabh Saksena | National Grid | NPCC | 1 |
| 19. | Michael Schiavone | National Grid | NPCC | 1 |
| 20. | Wayne Sipperly | New York Power Authority | NPCC | 5 |
| 21. | Tina Teng | Independent Electricity System Operator | NPCC | 2 |
| 22. | Donald Weaver | New Brunswick System Operator | NPCC | 2 |
| 23. | Ben Wu | Orange and Rockland Utilities | NPCC | 1 |
| 24. | Peter Yost | Consolidated Edison Co. of New York, Inc. | NPCC | 3 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2. | Group | Emily Pennel | Southwest Power Pool Regional Entity | | | | | | | | | | | X |

No additional members listed.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3. | Group | Chris Higgins | Bonneville Power Administration | X | | X | | X | X | | | | |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Forrest | Krigbaum | WECC | 1 |
| 2. | Nick | Choi | WECC | 1 |
| 3. | Mike | Miller | WECC | 1 |
| 4. | Erika | Doot | WECC | 3, 5, 6 |
| 5. | Stephen | Larson | WECC | 1, 3, 5, 6 |
| 6. | Peter | Raschio | WECC | 1 |
| 7. | Mark | Tucker | WECC | 1, 3, 5, 6 |
| 8. | Tedd | Snodgrass | WECC | 1 |
| 9. | Huy | Ngo | WECC | 1 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4. | Group | Connie Lowe | Dominion | X | | X | | X | X | | | | |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Greg Dodson | | SERC | 1, 3, 5, 6 |
| 2. | Mike Garton | | NPCC | 5, 6 |

| Group/Individual | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 3. Louis Slade | | RFC | 5, 6 | | | | | | | | | |
| 4. Michael Gildea | | MRO | 5, 6 | | | | | | | | | |
| 5. Group | David Thorne | Pepco Holdings Inc & Affiliates | X | | X | | | | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Michael | O'Grady | RFC | 1 | | | | | | | | | |
| 6. Group | Sam Ciccone | FirstEnergy | X | | X | X | X | X | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Troy Rhoades | FE | RFC | | | | | | | | | | |
| 2. M.J. Linn | FE | RFC | | | | | | | | | | |
| 3. Dough Hohlbaugh | FE | RFC | | | | | | | | | | |
| 7. Group | Dean Larson | Kansas City Power & Light | X | | X | | X | X | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Scott Harris | Kansas City Power & Light | SPP | 1, 3, 5, 6 | | | | | | | | | |
| 2. Michael Gammon | Kansas City Power & Light | SPP | 1, 3, 5, 6 | | | | | | | | | |
| 8. Group | Gregory Campoli | ISO/RTO Standards Review Committee | | X | | | | | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. Albert DiCaprio | PJM | RFC | 2 | | | | | | | | | |
| 2. Mark Thompson | AESO | WECC | 2 | | | | | | | | | |
| 3. Gary DeShazo | CAISO | WECC | 2 | | | | | | | | | |
| 4. Steven Myers | ERCOT | ERCOT | 2 | | | | | | | | | |
| 5. Ben Li | IESO | NPCC | 2 | | | | | | | | | |
| 6. Matt Goldberg | ISO-NE | NPCC | 2 | | | | | | | | | |
| 7. Bill Phillips | MISO | RFC | 2 | | | | | | | | | |
| 8. Donald Weaver | NBSO | NPCC | 2 | | | | | | | | | |
| 9. Charles Yeung | SPP | SPP | 2 | | | | | | | | | |
| 9. Group | Jason Marshall | ACES Power Marketing Collaborators | | | | | | X | | | | |
| **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. James Jones | AEPCO/SWTC | WECC | 1, 4, 5 | | | | | | | | | |
| 2. Shari Heino | Brazo Electric Power Cooperative | ERCOT | 1 | | | | | | | | | |
| 3. Michael Brytowski | Great River Energy | MRO | 1, 3, 5, 6 | | | | | | | | | |

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 4. | Bob Solomon | Hoosier Energy | RFC 1 | | | | | | | | | | |
| 10. | Group | Marie Knox | MISO Standards Collaborators | | X | | | | | | X | | |
| | **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. | Jim Cyrulewski | JDRJC Associates, LLC | RFC | 8 | | | | | | | | | |
| 11. | Group | Jesus Sammy Alcaraz | Imperial Irrigation District (IID) | X | | X | X | X | X | | | | |
| | **Additional Member** | **Additional Organization** | **Region** | **Segment Selection** | | | | | | | | | |
| 1. | Marcela Caballero | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 2. | Israel Gonzalez | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 3. | Peter Nguyen | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 4. | Mauricio Lopez | IID | WECC | 1, 3, 4, 5, 6 | | | | | | | | | |
| 12. | Individual | Sandra Shaffer | PacifiCorp | X | | X | | X | X | | | | |
| 13. | Individual | Shane Eaker | Southern Company | X | | X | | X | X | | | | |
| 14. | Individual | Kieth Morisette | Tacoma Public Utilities | X | | X | X | X | X | | | | |
| 15. | Individual | Keira Kazmerski | Xcel Energy | X | | X | | X | X | | | | |
| 16. | Individual | Jay Walker | NIPSCO | X | | X | | X | X | | | | |
| 17. | Individual | Ronnie Hoeinghaus | City of Garland | | | X | | | | | | | |
| 18. | Individual | Andrew Z. Pusztai | American Transmission Company, LLC | X | | | | | | | | | |
| 19. | Individual | Thad Ness | American Electric Power | X | | X | | X | X | | | | |
| 20. | Individual | Randi Nyholm | Minnesota Power | X | | X | | X | X | | | | |
| 21. | Individual | Greg Rowland | Duke Energy | X | | X | | X | X | | | | |
| 22. | Individual | Brian J Murphy | NextEra Energy Inc. | X | | X | | X | X | | | | |
| 23. | Individual | Michelle R D'Antuono | Ingleside Cogeneration LP | | | | | X | | | | | |
| 24. | Individual | Michael Falvo | Independent Electricity System Operator | | X | | | | | | | | |
| 25. | Individual | Kim Koster | MidAmerican Energy Company | X | | X | | X | X | | | | |
| 26. | Individual | Kirit Shah | Ameren | X | | X | | X | X | | | | |
| 27. | Individual | Jonathan Appelbaum | United Illuminating Company | X | | | | | | | | | |
| 28. | Individual | Jim Eckelkamp | Progress Energy | X | | X | | X | X | | | | |

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 29. | Individual | Andrew Ginter | Waterfall Security Solutions | | | | | | | | X | | |
| 30. | Individual | Thomas Johnson | Salt River Project | X | | X | | X | X | | | | |
| 31. | Individual | Andrew Gallo | Austin Energy | X | | X | X | X | X | | | | |
| 32. | Individual | Patrick Brown | Essential Power, LLC | X | | | | X | | | | | |
| 33. | Individual | John Seelke | PSEG (Public Service Enterprise Group) | X | | X | | X | X | | | | |
| 34. | Individual | Christina Bigelow | Midwest ISO | | X | | | | | | | | |
| 35. | Individual | Ron Donahey | Tampa Electric Company | X | | X | | X | X | | | | |
| 36. | Individual | Joe Doetzl | CRSI | X | | | | | | | | | |
| 37. | Individual | Darryl Curtis | Oncor Electric Delivery Company | X | | | | | | | | | |
| 38. | Individual | DANA SHOWALTER | E.ON CLIMATE & RENEWABLES | | | | | X | | | | | |

1. **The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on how a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement?**

**Summary Consideration:**

Most commenters agreed with the IDT that the request for interpretation asks for clarity on the meaning of a requirement. There were a few commenters that believe the request for interpretation is asking for clarity on the application, but the comments on the subject do not raise any significant issues that would affect the interpretation. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.

Some commenters suggested that the interpretation may cause difficulty in providing authorized access to vendors or contractors. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement andthe IDT must interpret a requirement according to the Guidelines for Interpretation Drafting Teams. The requirement language addresses "electronic access," and all electronic access must be authorized. Thus, regardless of a particular vendor's personnel screening or security training, any electronic access by that vendor's personnel, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The commenters also suggested that the issue should be addressed in conjunction with the CIP Version 5 development. The IDT notes that Project 2008-06 is working on Version 5 of the CIP standards, which is outside the scope of the IDT, and requests that commenters who suggested that the issue be addressed in Version 5 of the CIP standards provide specific suggestions when those standards are posted for comment.

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Midwest ISO | The request is asking for clarity on the meaning of | The request seeks clarification of the meaning of "authorized access." As a result, MISO submits that the request is asking for clarity on the meaning of the requirement as opposed to the application thereof. |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | a requirement. | |
| **Response: The IDT agrees that the request for interpretation asks for clarification on the meaning of a requirement.** | | |
| Ingleside Cogeneration LP | The request is asking for clarity on the meaning of a requirement. | WECC has requested a clarification of the definition of "authorized access" to determine if vendor personnel who provide supervised temporary support to Responsible Entities, are subject to CIP-004 R2 through R4. This is a subject of great relevance to Ingleside Cogeneration LP as we require all of our vendors to maintain robust cyber security programs, but agree with WECC that a literal reading of CIP-004 may require dedicated agents from each. Critical vendors such as Cisco or GE do not support an operating model like this - and we would argue that their security training and personnel screening procedures are superior. This subject will become especially prevalent when CIP Version 5 takes effect and all Responsible Entities will be required to have a cyber policy that addresses Cyber System Access. We would like to see this complex issue addressed now, before some precedence is set that proves to be uneconomical or unviable. |
| **Response: Thank you for your comment. The IDT must interpret a requirement according to the Guidelines for Interpretation Drafting Teams. The requirement language addresses "electronic access," and all electronic access must be authorized. Thus, regardless of a particular vendor's personnel screening or security training, any electronic access by that vendor's personnel, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT notes that Project 2008-06 is working on Version 5 of the CIP standards, which is outside the scope of the IDT. Therefore, the IDT recommends that the commentor provide specific suggestions to the Project 2008-06 SDT when the Version 5 CIP standards are posted for comment.** | | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| NextEra Energy Inc. | The request is asking for clarity on the application of a requirement. | Each of the three questions is asking whether a class of individuals (i.e., temporary vendors and supervisors of vendors) is required to comply with CIP-004 R2, R3 and R4. Thus, the questions are requesting specific confirmation whether one is or is out of compliance based on how these classes of individuals are addressed under CIP-004. |
| **Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement.** | | |
| Southwest Power Pool Regional Entity | The request is asking for clarity on the application of a requirement. | The clarification requested by WECC specifically states that the WECC RC seeks clarification on the definition of authorized access "as applied to temporary support from vendors." |
| **Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.** | | |
| MidAmerican Energy Company | The request is asking for clarity on the application of a requirement. | The request is asking for clarification on the application of the term “authorized access” in order to determine how to comply in the situation of temporary vendor support. |
| **Response: Thank you for your comment. While the IDT agrees that the interpretation has application implications, on balance, the IDT and most commenters agree that the interpretation is asking for clarity on the meaning of a requirement. The IDT** | | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| **believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.** | | |
| Northeast Power Coordinating Council | The request is asking for clarity on the meaning of a requirement. | |
| Dominion | The request is asking for clarity on the meaning of a requirement. | |
| FirstEnergy | The request is asking for clarity on the meaning of a requirement. | |
| ISO/RTO Standards Review Committee | The request is asking for clarity on the meaning of a requirement. | |
| ACES Power Marketing Collaborators | The request is asking for clarity on the meaning of a requirement. | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Imperial Irrigation District (IID) | The request is asking for clarity on the meaning of a requirement. | |
| NIPSCO | The request is asking for clarity on the meaning of a requirement. | |
| American Transmission Company, LLC | The request is asking for clarity on the meaning of a requirement. | |
| American Electric Power | The request is asking for clarity on the meaning of a requirement. | |
| Minnesota Power | The request is asking for clarity on the meaning of a requirement. | |
| Duke Energy | The request is asking for clarity | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | on the meaning of a requirement. | |
| Ameren | The request is asking for clarity on the meaning of a requirement. | |
| United Illuminating Company | The request is asking for clarity on the meaning of a requirement. | |
| Progress Energy | The request is asking for clarity on the meaning of a requirement. | |
| Waterfall Security Solutions | The request is asking for clarity on the meaning of a requirement. | |
| Salt River Project | The request is asking for clarity on the meaning of a requirement. | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Essential Power, LLC | The request is asking for clarity on the meaning of a requirement. | |
| PSEG (Public Service Enterprise Group) | The request is asking for clarity on the meaning of a requirement. | |
| Tampa Electric Company | The request is asking for clarity on the meaning of a requirement. | |
| CRSI | The request is asking for clarity on the meaning of a requirement. | |
| Oncor Electric Delivery Company | The request is asking for clarity on the meaning of a requirement. | |
| E.ON CLIMATE & RENEWABLES | The request is asking for clarity | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | on the meaning of a requirement. | |
| Bonneville Power Administration | The request is asking for clarity on the application of a requirement. | |
| Pepco Holdings Inc & Affiliates | The request is asking for clarity on the application of a requirement. | |
| Kansas City Power & Light | The request is asking for clarity on the application of a requirement. | |
| MISO Standards Collaborators | The request is asking for clarity on the application of a requirement. | |
| PacifiCorp | The request is asking for clarity on the application of a requirement. | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| Southern Company | The request is asking for clarity on the application of a requirement. | |
| Tacoma Public Utilities | The request is asking for clarity on the application of a requirement. | |
| Xcel Energy | The request is asking for clarity on the application of a requirement. | |
| City of Garland | The request is asking for clarity on the application of a requirement. | |
| Independent Electricity System Operator | The request is asking for clarity on the application of a requirement. | |
| Austin Energy | The request is asking for clarity | |

| Organization | The Request is Asking for Clarity on the Meaning or Application of the Requirement | Question 1 Comment |
|---|---|---|
| | on the application of a requirement. | |
| **Response: Thank you for your comments.** | | |

**2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard?**

**Summary Consideration:**

Most commenters agree with the IDT that the interpretation does not expand the reach of the requirement, and one commenter expressed rationale that supports the IDT's interpretation by noting that allowing for the concept of supervised electronic access would expand the reach of the requirement.

One commenter believes that the interpretation expands the reach of the requirement because it uses references to standards that are not part of the standard being interpreted. The commenter suggests that such a reference would set an unacceptable precedent. In response to that concern, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors. That commenter also suggests that the interpretation reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is for physical access. However, the IDT notes that the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.

Some commenters do not believe the interpretation allows for emergency access when needed, or that the interpretation will make getting support from contractors difficult. The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.

Commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES.

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Omaha Public Power District | Negative | 1. The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the application of a requirement? 0 The request is asking for clarity on the meaning of a requirement. 1 The request is asking for clarity on the application of a requirement. Comments: N/A 2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard? 1 The interpretation expands the reach of the standard. 0 The interpretation does not expand the reach of the standard. Comments: OPPD respectfully disagrees with the proposed interpretation provided by NERC in response to questions submitted by WECC. Utilizing standards that are not in direct relation to the question being proposed contains no true definition or answer. This type of response sets an unacceptable precedence of using different standards and requirements to justify an interpretation. 3. Do you agree with this interpretation? If not, please explain specifically what you disagree with. 0 Yes 1 No Comments: In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | | Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, OPPD does not believe the interpretation allows for emergent electronic access when needed. OPPD believes there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, OPPD feels the risk level to the BES, in terms of reliability, is indeed increased. |
| **Response: -In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.**<br>**-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br>**-The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.** | | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| -Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. | | |
| Bonneville Power Administration | The interpretation does not expand the reach of the standard. | BPA believes that if the drafting team allowed for the concept of supervised cyber access, they would be expanding the scope CIP-004. |
| Response: Thank you for the comment and supporting rationale that reinforces the IDT's interpretation. | | |
| Northeast Power Coordinating Council | The interpretation does not expand the reach of the standard. | |
| Southwest Power Pool Regional Entity | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Pepco Holdings Inc & Affiliates | The interpretation does not expand the reach of the standard. | |
| FirstEnergy | The interpretation does not expand the reach of the standard. | |
| Kansas City Power & Light | The interpretation does not expand the reach of the standard. | |
| ISO/RTO Standards Review Committee | The interpretation does not | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | expand the reach of the standard. | |
| Imperial Irrigation District (IID) | The interpretation does not expand the reach of the standard. | |
| PacifiCorp | The interpretation does not expand the reach of the standard. | |
| Tacoma Public Utilities | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Xcel Energy | The interpretation does not expand the reach of the standard. | |
| NIPSCO | The interpretation does not expand the reach of the standard. | |
| American Transmission Company, LLC | The interpretation does not expand the reach of the standard. | |
| American Electric Power | The interpretation does not | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | expand the reach of the standard. | |
| Minnesota Power | The interpretation does not expand the reach of the standard. | |
| Duke Energy | The interpretation does not expand the reach of the standard. | |
| Independent Electricity System Operator | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Waterfall Security Solutions | The interpretation does not expand the reach of the standard. | |
| Salt River Project | The interpretation does not expand the reach of the standard. | |
| Austin Energy | The interpretation does not expand the reach of the standard. | |
| Essential Power, LLC | The interpretation does not | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | expand the reach of the standard. | |
| PSEG (Public Service Enterprise Group) | The interpretation does not expand the reach of the standard. | |
| Tampa Electric Company | The interpretation does not expand the reach of the standard. | |
| CRSI | The interpretation does not expand the reach of the standard. | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| Oncor Electric Delivery Company | The interpretation does not expand the reach of the standard. | |
| E.ON CLIMATE & RENEWABLES | The interpretation does not expand the reach of the standard. | |
| MISO Standards Collaborators | The interpretation expands the reach of the standard. | |
| Southern Company | The interpretation expands the reach of the | |

| Organization | Yes or No<br>The Interpretation Expands/Does Not Expand the Reach of the Standard | Question 2 Comment |
|---|---|---|
| | standard. | |
| Ameren | The interpretation expands the reach of the standard. | |
| United Illuminating Company | The interpretation expands the reach of the standard. | |
| Progress Energy | The interpretation expands the reach of the standard. | |
| **Response: Thank you for your comments.** | | |

**3. Do you agree with this interpretation? If not, please explain specifically what you disagree with.**

**Summary Consideration:**

The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation. After considering the comments, the IDT decided not to make any changes to its interpretation, and explains its rationale in response to the concerns raised by commenters below.

One commenter does not believe that the standard separates how to treat cyber and physical access for vendors with regard to supervision, but the IDT notes that the standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.

Some commenters noted that training alone will not prevent a vendor from perpetrating malicious activity. In response, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and this is not supported by the language in the requirement. The standard language (and the interpretation) does not prevent supervised access; however, all electronic access must be authorized pursuant to the requirements in CIP-004. Modification of the standard to allow such electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.

Another commenter agreed with the interpretation while noting that the interpretation may confirm a logistical problem in getting vendor support when a vendor will not submit to the entity's background checks and training. This is a point that the IDT addressed in development discussions, and it determined that it is outside the scope of an interpretation. The greater standards development process is better equipped to weigh those concerns, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT understands that the Version 5 CIP SDT is aware of this logistics concern. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.

A commenter supported the IDT's rationale by noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent harm, and that granting direct cyber access inhibits that ability.

A commenter in agreement with the overall interpretation suggested that the reference to "authorized access" might be made clearer if, rather than referencing R2, R3, and R4, the interpretation specifically stated what those requirements are. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as

requested by the request for interpretation. The IDT also considered the approach of fully stating the requirements, but notes that upon approval, this interpretation will be appended to the standard itself, and R2, R3, and R4 will be easy to reference.

Several commenters noted concern that the interpretation may increase risk to the BES, but considering the provisions for emergency and planned access, the IDT does not believe this interpretation increases the risk level to the BES. Furthermore, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams.

Commenters suggested that the absence of language regarding supervision or escorting with respect to electronic access does not absolutely prohibit the concept. In response, the IDT notes the requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Some commenters also suggest that the standards should be modified to allow for vendor or contractor access without having to satisfy the authorization requirements. However, modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT believes that the interpretation adequately addresses that all cyber access is contemplated by the interpretation, which includes both employees and vendors.

Commenters suggest that the intent of the standard was to allow supervised/escorted cyber access. The IDT does not find support in the language of the standard that "the intent of the standard is to allow for supervised/escorted access for both physical and cyber access." Additionally, some commenters believe the interpretation does not allow for necessary emergency access, or that the interpretation will make getting support from contractors difficult. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements.

Commenters suggest that the interpretation defines or puts bounds on the definitions of "authorized access", "cyber access", and "physical access" and that the interpretation equates "authorized access" with being on the list under CIP-004-1, Requirement R4. The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed.

Other commenters suggest 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, the IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. Furthermore, there are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).

Commenters suggest that if a Responsible Entity can demonstrate that they can supervise remote cyber access, then that access should be allowed. The IDT believes that the relevant question to resolve is not whether an entity can supervise remote cyber access, but whether such access is allowed by the standard. The requirement language addresses "electronic access," and all electronic access must be authorized.

Commenters suggest that since "authorized access" is not in the standard, use of the phrase in the interpretation expands the reach of the standard. In response, the IDT notes that it sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.

Some commenters noted concern that the interpretation's reference of other standards sets a bad precedent, but the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.

One commenter agrees with the conclusion of the interpretation, but believes that the request for interpretation is asking for compliance guidance and that the interpretation only restates information in the standard. While the IDT agrees that the interpretation has compliance application implications, on balance, the IDT and most commenters agree that the interpretation is validly asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| Alberta Electric System Operator | Abstain | The AESO agrees with the interpretation of CIP-004, however we are casting an abstain vote as this standard is not applicable in Alberta at this time. |
| **Response: Thank you for the comment.** | | |
| Consolidated Edison Co. of New York | Affirmative | See NPCC region-wide group comment form |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: See NPCC response** | | |
| California ISO | Affirmative | Comments form provided jointly with ISO/RTO Standards Review Committee |
| **Response: See ISO/RTO response** | | |
| Electric Reliability Council of Texas, Inc. | Affirmative | ERCOT ISO has joined the comments of the ISO/RTO Council Standards Review Committee. |
| **Response: See ISO/RTO response** | | |
| Midwest ISO, Inc. | Affirmative | We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access. |
| **Response:**<br>"We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision."<br>**The standard language treats electronic and physical access separately by including the word "unescorted" in conjunction with physical access; it does not use "unescorted" in reference to electronic access.**<br>"The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity."<br>**Whether temporary or permanent, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br>"Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access." | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **The IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and this is not supported by the language in the requirement. The standard language (and the interpretation) does not prevent supervised access; however, all electronic access must be authorized pursuant to the requirements in CIP-004. Modification of the standard to allow such electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Cowlitz County PUD | Affirmative | The interpretation is correct. However it does confirm a logistical problem: how to obtain vendor support when the vendor will not submit to the entity's requirement for background checks and training. If the cyber system is broken and can only be fixed via vendor support, the time to get an Exception approved or replace the cyber asset could have a serious negative impact on the BES. |
| **Response: Thank you for the comment. This is a point that the IDT addressed in development discussions, and it determined that it is outside the scope of an interpretation. The greater standards development process is better equipped to weigh those concerns, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT understands that the Version 5 SDT is aware of this logistics concern. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.** | | |
| Wisconsin Energy Corp. | Affirmative | Comments are requested to be submitted using the separate electronic comment form rather than with the vote. While the answer gets a bit circular, and there is room for disagreement in the industry on the interpretation, I support it and do not have any specific comments to submit with this vote. |
| **Response: Thank you for your comment.** | | |
| Southwest Power Pool Regional Entity | Yes | The SPP RE agrees with the interpretation, noting that the primary purpose of the escort is to be able to supervise and be able to intervene to prevent the escorted individual from overtly, covertly, or inadvertently causing harm. Granting direct cyber access to someone without authorized access inhibits the ability to perform |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | the escort responsibilities and introduces risk. As noted in the interpretation, this is why the standard specifically makes a distinction regarding "authorized, unescorted" physical access. Technically, escorted cyber access is not feasible. The SPP RE agrees that "over the shoulder" viewing via a webinar or close proximity presence, while possibly subject to the entity's CIP-003/R5 information protection program, does not constitute cyber access. |
| **Response: Thank you for the comments and rationale, which supports the IDT's interpretation.** | | |
| Tacoma Public Utilities | Yes | Agree with the standard as written in the WECC position paper |
| **Response: Thank you for the comment.** | | |
| American Electric Power | Yes | AEP agrees with the overall interpretation, but offers the following commentsand recommendations for improving the interpretation.Responses to Questions 1 and 2:The response provided for Q1 does not definitively answer the question that was posed. The question posed asks what the definition is for "authorized access", while the response essentially states that one has this access by being on the proper list. It is not clear from the response how those on the authorized list were added to it, i.e. that those individuals met the necessary training, risk assessment, and access requirements. This might be made clearer if, rather than generally mentioning R2, R3, and R4, specifically stating what those requirements are.The response provided for Question 2 more adequately addresses Question 1 than does the response to Q1. |
| **Response: Thank you for your comments. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as requested by the request for interpretation. The IDT also considered the approach of fully stating the requirements, but notes that upon approval, this interpretation will be appended to the standard itself, and R2, R3, and R4 will be easy to reference.** | | |
| PSEG (Public Service Enterprise Group) | Yes | The inability to provide Escorted Cyber Access through a web-conference (or otherwise), can be detrimental to the reliability of the BES as the time to |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | troubleshoot cyber/networking issues can be extensive without letting the remote support personnel have access to the troubled device. |
| **Response: Thank you for your comment. The IDT understands this concern, but notes that the greater standards development process is better equipped to review such a concept, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Additionally, given the provisions for emergency access and the ability to plan in advance for authorizing access, the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| Tampa Electric Company | Yes | Although we believe that the Interpretations Drafting Team has correctly provided the interpretation, we believe that the standard should be changed to provide a vehicle for emergency vendor access via cyber or physical escorting. The lack of the ability to provide this emergency access could be detrimental to the reliability of the grid and may force Entities into non-compliance to meet the emergency situation. |
| **Response: -Thank you for your comments. The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to BES reliability. Considering those provisions for emergency and planned access, the IDT does not believe this interpretation is detrimental to reliability.**<br>**-The IDT notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.** | | |
| Oncor Electric Delivery Company | Yes | Oncor Electric Delivery agrees with this interpretation. The interpretation provides greater clarity on how a Compliance Enforcement Agency (CEA) addresses "cyber access" which includes both physical and remote acc |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: Thank you for your comments** | | |
| Dominion | The interpretation expands the reach of the standard. | The lack of an expression such as “escorted electronic access” does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard. |
| **Response: The requirement language addresses “electronic access,” and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of “escorted” supervision for individuals with electronic access, it does not include a provision for “escorted” cyber access. Thus, any electronic access, whether “escorted” or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| ACES Power Marketing Collaborators | The interpretation expands the reach of the standard. | Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines “authorized access’ by stating that an individual has “authorized access” if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated “authorized access” with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since Console access is almost always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device. |
| **Response: The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. There are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).** | | |
| NextEra Energy Inc. | The interpretation expands the reach of the standard. | It could be viewed that the interpretation requested tends to expand the reach of CIP-004, given the lack of clarity in the answers. Thus, if this interpretation goes forward, it is recommended that that the following clearer and more to the point answers be substituted for the current answers, so there is no expanding of CIP-004 nor an elaboration on how the standard applies to particular facts:1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors. Answer: The term authorized access as used in CIP-004 is not limited or qualified by any type or class of employees or vendors. Thus, all employees and vendors (who desire either physical or cyber access) without regard to whether they are temporary support or not must either: (1) be escorted by someone with authorized unescorted physical or authorized cyber access, as applicable or (2) have been granted authorized unescorted physical or authorized cyber access by meeting the requirements of R2 and R3. Thus, there is no exception for temporary support from vendors, and the term authorized access applies to them in the same manner it applies to any other class or type of employee or vendor. 2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?Answer: Yes. The language of CIP-004 applies to all employees and vendors that desire |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | unescorted physical or cyber access to Critical Cyber Assets without regard to whether or not the employee or vendor is supervised. 3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision? Answer. See answer to question 2 - supervised vendors are not exempt from CIP-004-1, Requirements R2, R3, and R4, thus the remainder of the question is moot. |
| **Response: The IDT considered these suggestions. The IDT believes that the interpretation adequately addresses that *all* cyber access is contemplated by the interpretation, which includes both employees and vendors. The IDT does not fully agree with the suggested phrase, "be escorted by someone with authorized unescorted physical or authorized cyber access" with respect to CIP-004, versions 2 through 4, and believes that it only exists in version 1 with respect to the 30 and 90 day periods acknowledged in the interpretation's footnote.** | | |
| Ingleside Cogeneration LP | The interpretation expands the reach of the standard. | The project team has chosen to differentiate between escorted physical access where a vendor performs a non-cyber activity (such as replacing parts) from one where a cyber connection has been made. Ingleside Cogeneration LP believes the project team has read in extra language into the requirement - and changed FERC's intent in Order 706 paragraph 432. That paragraph was cited by WECC in the original Request for Interpretation, and clearly acknowledges that supervised access is a real-life operational need under certain circumstances. If anything, the Commission brings up a good point about the qualifications of the escort, but it does not seem appropriate that the drafting team has completely ruled out supervised cyber access. Furthermore, by logical inference, if the Responsible Entity can demonstrate that they can supervise remote cyber access, then that should be allowed as well. |
| **Response: The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT is interpreting the standard language as approved by FERC, and its interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** | | |
| MidAmerican Energy Company | The interpretation expands the reach of the standard. | WECC is seeking "clarification on the definition of 'authorized access.'" |
| **Response: Thank you for your comments. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition, and the IDT sought to provide clarity on the term as requested by the request for interpretation.** | | |
| Midwest ISO | The interpretation expands the reach of the standard. | MISO respectfully submits that, based on a literal reading of the plain language of CIP-004, the phrase "authorized access" is not part of the language of the requirement requested for interpretation. The use of a specific term not utilized in the requirement as well as the assignment of a specific meaning and obligations from the requirement at issue to such a term by the Interpretation Drafting Team ("IDT") in its Interpretation expands the reach of the standard. |
| **Response: The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.** | | |
| Pacific Gas and Electric Company | Negative | PG&E disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or on-site cyber access). Registered entities should be allowed to provide vendors, which they have engaged, with temporary digitally escorted access. Prohibiting this capability directly affects the safe and reliable operations of the Bulk |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | Electric System. If this interpretation is approved as worded, a valuable support tool could place utilities in a position where reliability suffers to maintain compliance. Let's take one of the well know router companies for example. This company has one of the highest performing Tier 1 support record of any company. When you call their support you reach their Tier 1 support desk which if allowed to be escorted digitally can address most issues within a reasonable timeframe. If escorted digital access is prohibited entities would have to negotiate dedicated Cisco technicians to support their devices. Not only would this be extremely costly, if possible, most importantly it would not be efficient resulting in delays to address the issue at hand. For remote access, technologies such as WebEx, TightVNC, Timbuk2, etc enable strict remote control solutions, this allows someone to provide logical remote control to a system while fully recording and visually observe (e.g., digitally escort) all actions. At any time, the escort observes anything inappropriate they can shut-off access immediately by a click of a button. In reality, allowing, "digital escorting" is much safer than allowing someone physical access to critical assets as the escort can stop any action with a click of a button whereas with physical access the "escort" has to have the capability to physically stop the individual. For on-site cyber access entities should be able to perform these activities in the same manner that they provide escorting to other visitors, through visual observation. Someone with escorted physical access can do more physical damage to critical assets faster than they can do damage typing on a keyboard with an escort observing them. For example, if the escort observes anything inappropriate being typed they can physically interrupt the individual and keep them from hitting the "enter/execute" command; however, someone can grab a handful of fiber cables going into a patch panel and yank them out before an escort could stop them. |
| **Response: The IDT does not find support in the language of the standard that "the intent of the standard is to allow for supervised/escorted access for both physical and cyber access." The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to BES reliability or safety.** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Considering those provisions for emergency and planned access, the IDT does not believe this interpretation is detrimental to reliability. The IDT also notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 standards are posted for comment.** | | |
| Salt River Project | Negative | The interpretation does not clearly define that escorted electronic access is prohibited. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| Brazos Electric Power Cooperative, Inc. | Negative | See comments provided by ACES Power Marketing. |
| **Response: See ACES response** | | |
| Southwest Transmission Cooperative, Inc. | Negative | Contrary to the standards development process, the interpretation either defines or places bounds on the definition of three terms: authorized access, cyber access and physical access. The interpretation defines "authorized access' by stating that an individual has "authorized access" if they are on the list developed pursuant to CIP-004-1 Requirement R4. Thus, the interpretation has equated "authorized access" with being included on this list. The interpretation also equates typing at a keyboard interface of a Critical Cyber Asset within the Physical Security Perimeter as cyber access. By equating this as cyber access, the definition of physical access has been bounded to prevent it from including this escorted access. It would be reasonable for a registered entity to consider an escorted vendor accessing a Critical Cyber Asset (i.e. typing at the keyboard interface) from within the Physical Security Perimeter as physical access. After all, the individual is being given temporary physical access (i.e. identity check, visitor badge, entry in the visitor control program) and they are not given temporary cyber access (i.e. temporary account, log-in credentials). Since |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | Console access is almost always included in the physical security section of computer security manuals, this is a reasonable interpretation, and there is nothing in the standard that prevents this reasonable interpretation of physical access. Furthermore, escorted physical access loses any meaning and would no longer be a necessary term in the standard if escorted physical access did not allow physical interaction with the device. This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | to the interpretation, most (probably all) registered entities have a formal process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed. We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert,software expert). |
| **Response: -The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted"** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT does not dispute that typing on a keyboard or console access is physical access, but it is also electronic access. There are a number of contexts in which someone would need escorted physical access yet is not interacting electronically with a device, such as any facility work (e.g., HVAC, fire alarm, maintenance work, etc).**<br><br>**-The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. The IDT is interpreting the standard language as approved by FERC, and its interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."**<br><br>**-Modification of the standard to allow electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. However, the CIP IDT encourages the commenter to provide specific suggestions to address this issue when the Version 5 CIP standards are posted for comment.** | | |
| Central Lincoln PUD | Negative | The interpretation effectively disallows vendor cyber access, since vendors will be unwilling to undergo training established by each of their customers. The resulting lack of support will add risk to the BES. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| City and County of San Francisco | Negative | While in theory we believe the interpretation makes sense, its real world application is likely to result in undesirable consequences with respect to vendor support of control system maintenance, and have a negative impact on BES reliability. We believe that the concept of requiring a responsible Entity to have document that its vendor has personnel risk assessment program and cyber security training may be |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | worth exploring. |
| **Response: -The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.** | | |
| Essential Power, LLC | Negative | Comments: In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation. In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support. Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard. There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. The IDT encourages the commenter to provide specific suggestions for addressing this issue when the Version 5 CIP standards are posted for comment.** | | |
| Salt River Project | Negative | As written the interpretation does not clearly define that escorted electronic access is prohibited. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| U.S. Army Corps of Engineers | Negative | In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, we do not believe the interpretation allows for emergent electronic access when needed. Many companies believe there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, the risk level to the BES, in terms of reliability, is increased. |
| **Response: Response: -While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br><br>**-In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.**<br><br>**-The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| Salt River Project | Negative | The interpretation does not clearly provide a definition that escorted electronic access is prohibited. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| Dominion | No | The following Dominion responses are provided in order of the questions asked by WECC:1. The interpretation that individuals on the list of personnel authorized for cyber or unescorted physical access to CCAs are subject to CIP-004-1 R2, R3 (with allowed restrictions), and R4 is appropriate.2. CIP-004-1-R4 specifically addresses authorized access and does not state that "all cyber access to Critical Cyber Assets must be authorized". CIP-004-1-R2 and CIP-004-1-R3 (with allowed restrictions) apply to "personnel having authorized cyber or authorized unescorted physical access". The lack of an expression such as "escorted electronic access" does not exclude or prohibit the concept, it's simply unaccounted for within the standard. Any interpretation that would include or exclude concepts which are not already addressed by a standard ultimately expands the reach of the standard.3. The concept of "escorted electronic access" is absent from CIP-004-1. Absent a standard, it should be up to each Registered Entity to determine by internal policy whether or not escorted electronic access should be allowed. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.** | | |
| Pepco Holdings Inc & Affiliates | No | It is understood why the SDT applied a strict interpretation which results in no change to the existing standard. The requested interpretation would have changed the meaning and reach of the standard. However there still remains a very serious real problem. There is a need to allow cyber access to a vendor on some sort of an emergency basis without meeting R2 and R3. The Impact Statement in the Request for Interpretation submitted by WECC is a very serious problem for many entities that could result in a high risk or serious system reliability problem. |
| **Response: The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| FirstEnergy | No | There is an inherent flaw in the interpretation because it is based on an inactive standard CIP-004-1. The current effective standard is CIP-004-3 which differs in a significant way from CIP-004-1. Version 3 of this standard now allows exceptions in emergency situations as stated from the phrase "except in specified circumstances such as an emergency" which is included in R2.1 and R3. This specifically affects the answer to WECC's third question. Remote and on-site cyber access should be allowed under supervision during emergency situations and it would be very difficult to assure that all personnel offering remote assistance in these situations were assessed per the requirements of CIP-004.A second inherent flaw is that the interpretation is based on an inactive standard CIP-006-1. The current effective standard CIP-006-3 expressly describes visitor supervision requirements. Per CIP-006-3, R1.6, visitors are required to be continuously escorted within Physical Security Perimeters. This revised requirement should be integrated into the answers to WECC's second and third question.Therefore, we suggest the team revise the interpretation to only make reference to the current Version 3 standards, and add language in the interpretation that there are exceptions for emergency situations as specified by the entity per CIP-003 which requires details of those emergency situations. |
| **Response: The IDT considered all versions of the CIP standards throughout the Interpretation process as entities could still undergo audit proceedings to CIP Version 1. When an interpretation is requested for an ealier version of a standard, and the issue for which interpretation is requested persists in subsequent versions, the interpretation applies to all of the versions of the standard in which the language being interpreted exists. With regard to the emergency exceptions, the IDT notes that CIP Version 1 allowed for a 30 and 90 day provision with respect to Personnel Risk Assessments and Training. Through the Standards development process this language was removed and replaced with language in CIP Version 2 (which is retained in subsequent approved versions) to allow exceptions to the training and personnel risk assessment authorization requirements in specified** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **circumstances, including emergency situations.** | | |
| ACES Power Marketing Collaborators | No | This interpretation will decrease reliability. Many large vendors simply are not going to subject their employees to a registered entity's training program as this interpretation would require because their employees are already experts and thoroughly understand that they can impact their customer's operations negatively. Additional training from the registered entity will not further enforce this understanding. Thus, maintenance will be slowed or delayed. If a registered entity employee must enter all commands (rather than allowing the vendor to enter the commands) that will slow the process down because the vendor could simply do it faster. Slowing down maintenance could cause other maintenance to be delayed. Maintenance could also be delayed because the vendor is willing to complete the registered entity's training program but these tasks are not completed in time for the maintenance. Ultimately, delayed maintenance leads to real-time operating issues and emergencies which ironically are allowed exceptions in the standards. Thus, the interpretation could force a registered entity into a position of performing emergency maintenance. Three terms are defined or bounded outside the standards development process. These terms include: authorized access, cyber access and physical access. We will not repeat our arguments regarding this expansion of the standard here. They can be found in question 2. The interpretation applies flawed circular logic for what constitutes authorized access. It states that because CIP-004-1 R4 requires the applicable registered entity to "maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets" a person has "authorized access" if they are on that list. It further states that those individuals that are on this list would then be subject to CIP-004-1 R2, R3 and R4. This logic is faulty for several reasons. First, it requires that a registered entity could never violate CIP-004-1 R4 since the list of personnel with access is being treated as the official record of those with "authorized access". If they are not on the list, the logic presumes they do not have "authorized access". Second, the logic presumes that there are no other registered entity processes that grant authorized access. Contrary to the interpretation, most (probably all) registered entities have a formal |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | process to grant "authorized access" that requires management sign off at various levels. Management is in fact who is authorizing access and not a list of record. Third, this logic assumes that the lists of personnel with "authorized access" cannot be in error or it is somehow impossible to actually have access without being on this list. This access list is really a log or diary of all individuals who are supposed to have "authorized access" but it could be flawed.We believe this interpretation is inconsistent with Order 706. Paragraph 431 states that limited exceptions should be allowed for the need for all individuals to complete the registered entity's training program. While emergencies are listed as one exception example and are included in the standard as an exception, there is no other language in the FERC order that states emergencies should be the only limited exception. We believe vendors that are unwilling to complete the registered entity's training program represent another reasonable exception. In contradiction, the interpretation limits the registered entity's ability to utilize this exception which is allowed by the FERC Order 706. Paragraph 432 further clarifies and supports this position in that it allows newly hired employees or vendors to be granted access before completing training if they are escorted by an individual that possesses sufficient expertise regarding the Critical Cyber Asset to ensure the actions of the vendor or newly hired employee do not harm the Critical Cyber Asset. Given that FERC did not limit the actions that the vendor could take and simply required the escort to have sufficient knowledge to prevent harm, we believe FERC fully expected that the vendor may be inputting commands to the Critical Cyber Asset and not just manipulating the hardware as the interpretation envisions. FERC's statement of sufficient knowledge would imply that the knowledge of the escort must match the situation (i.e. hardware expert, software expert). |
| **Response: -The IDT notes Version 2 and subsequent versions of the CIP standards allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations, which is consistent with FERC Order No. 706, Paragraph 431. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| -The IDT notes that the FERC Order No. 706 issued directives for development of the CIP standards, and the approved standards that resulted from consideration of Order No. 706 are the relevant requirements that are mandatory and enforceable on Responsible Entities under a particular standard. FERC Order No. 706 itself does not create or allow an exception to a reliability standard. Furthermore, the IDT disagrees that Paragraph 431 merely directs that "limited exceptions should be allowed"; rather, Paragraph 431 suggests that the limited exceptions to required training before obtaining access relate to specific conditions, "such as during emergencies, subject to documentation and mitigation." (FERC Order No. 706, Paragraph 431). That is consistent with the IDT's recognition of the provisions for emergency and planned access.<br>-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.<br>-With regard to the emergency exceptions and FERC Order No. 706, the IDT notes that CIP Version 1 allowed for a 30 and 90 day provision with respect to Personnel Risk Assessments and Training. Through the Standards development process this language was removed and replaced with language in CIP Version 2 and beyond to allow exceptions to the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations.<br>-In response to the comments submitted in regard to an entity's list, maintenance of a list, management approval processes, and list inconsistencies with actual physical and cyber access controls, the IDT cannot make interpretations on how specific entities are achieving compliance. The IDT understands the concerns raised by the commenter, however the IDT understands that each entity has unique processes for achieving and demonstrating compliance. | | |
| Southern Company | No | Comments: Question 2 and 3 from the Request for Interpretation are not answered by the interpretation. The answers simply describe how the CIP standards do not address the questions being asked. The standards do not address the scenario contemplated by the line of questioning and should be remanded to the CIP SDT to fix in version 5 of the standards.Comment:Vendor support personnel dispatched to the various generation sites are selected base upon their physical availability and the expertise required on the projects. It is a difficult task to provide ongoing training and background checks for every potential individual from numerous vendors supporting a variety of systems. It is near impossible to monitor the ongoing employment status of this large number of vendor personnel, to assure timely removal from the access control list, that will be required if implemented as discussed in the proposed interpretation.At present, vendor personnel supplying |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | setup/support may work freely on pre-shipped non-installed systems. This trusted relationship should be extended, to similar individuals under escort at the equipment site. If the support function requires that changes be made to systems, having site personnel follow the direction of the vendor expert presents an increase potential for error, while adding marginal security benefits. |
| **Response: Thank You for your comment. The IDT must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation. Modifications to an approved Standard must be addressed within the Standards development process, the IDT encourages the commenter to submit the comments to the SDT working on CIP V5.** | | |
| City of Garland | No | Disagree with the concept of there being no escorted Cyber Access. If someone with authorized access is working with a vendor or contractor on an issue, the system is more secure than if you give him authorized access just because he has a PRA and has had CIP training. Take for example, Hector Xavier Monsegur, the notorious hacker known as Sabu and leader of LulzSec. Because of his cooperation and work with the FBI and other agencies, he may end up with his record cleansed or at least be able to put on a resume his work with the FBI. Eight years from now, a 7 year criminal background check could be clear. If a company were to utilize him for a short term issue, would the company be more secure with him being "escorted" or with him being issued authorized access and allowed free access. It is noted in your supporting comments that the standard requirements do not state specifically that escorted cyber access is permitted. On the other hand, the standard requirements do not have statements preventing escorted cyber access either. Which is more secure? |
| **Response: -Thank You for your comment. While the effectiveness of personnel risk assessment and Training controls are an interesting theoretical discussion, the IDT must provide an interpretation that meets the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| -While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. | | |
| NextEra Energy Inc. | No | As written, this interpretation should either be dismissed as in appropriate or the answers re-written to be clearer and more responsive. See answers to question 1 and 2. |
| Response: Thank you for your comment. See response to commenter in Question 2. | | |
| Ingleside Cogeneration LP | No | Ingleside Cogeneration LP believes that the interpretation is an overly-literal reading of CIP-004 and may hamper routine technical support processes with no demonstrable reduction in cyber-risk . The power and convenience of remote vendor maintenance may be unavailable to all but the largest utilities should costs rise because of it. Such a result will actually diminish BES reliability as access to highly competent technical support and maintenance personnel becomes restricted.There may be acceptable solutions, however. It would seem that a single cyber certification of vendors such as Cisco and GE could be referenced in thousands of individual security policies. Alternatively, the industry could provide a single generic cyber training package and employee background check method for vendors. We would hope that NERC takes a leadership position in resolving these complex issues.Lastly, the industry needs more direction than that provided in the circular response to the first question. The project team essentially states that the Responsible Entity must determine who has authorized access to their Critical Cyber Assets and include them on an access list. That list will then define authorized access - leaving the door open for a wide variety of resolutions. |
| Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES. | | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **-The IDT understands this concern, but notes that the greater standards development process is better equipped to review such a concept, as revising a standard is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."<br>-The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed.** | | |
| MidAmerican Energy Company | No | The request is asking how to comply with one or more requirements in a specific situation with vendor support. Requests as to how to comply, per the Rules of Procedure, do not meet the valid criteria of an interpretation request. While we agree with the conclusion in the proposed response, the draft response restates information that already is in the standard. |
| **Response: The WECC RFI is seeking interpretation of a requirement, and the IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard. While the IDT agrees that the interpretation has compliance application implications, on balance, the IDT and most commenters agree that the interpretation is validly asking for clarity on the meaning of a requirement. The IDT believes that the illustration of temporary support from vendors was provided as an example of why further clarity is needed in order to help the industry understand this requirement.** | | |
| Ameren | No | The CIP-004 R4 IDT interpretation relies on incorrect logic in stating that Standard does not allow for escorted (supervised) cyber access to cyber assets solely because "unescorted cyber" is not explicitly included in the CIP-004 R4 "list". We agree with the idea put forth in the Requirement that anyone with unfettered cyber access is a potential danger and in like manner, so would anyone with unescorted physical access. However, the reason the Requirement does not require those with escorted cyber access to be listed is not because such access is somehow not contemplated or not permitted but rather because, like escorted physical access, these individuals, and their actions, are well monitored and controlled and do not need the extra care and handling that ensues from being on "The List" for those free to take independent action. The mere fact that they do not need further "handling" does not mean in any way that they do not exist or that this in not permitted. We are concerned that IDT is |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | using a classic argument from the negative to imply something is impermissible on that such use is not contemplated merely because it is absent from a list of threat types that need to be addressed. |
| **Response: While the IDT agrees that Requirement R2 does not explicitly deny the concept of "escorted" supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. The IDT also notes that changing the standard is outside the IDT's scope, as the "Guidelines for Interpretation Drafting Teams" specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** | | |
| United Illuminating Company | No | The Interpretation DT correctly states that CIP-004 R2 and R3 apply to individuals on a list designating them with authorized cyber access or authorized unescorted physical access to Critical Cyber Assets. The Interpretation DT makes an error in stating that CIP-004 limits the type of cyber access to a Critical Cyber Assets to only authorized individuals, that is, there is no opportunity to implement supervised remote access via terminal session (i.e. Webex) to support personnel not on the authorized cyber access list.The Reliability standards do not provide a definitive statement of the types of access allowed to Critical Cyber Assets. The Standards only provide the program requirements for three types of access; authorized physical, escorted physical, and authorized cyber. By not providing a definitive list of the types of access the original Drafting team did not exclude the type of access under review in this interpretation, that is, supervised cyber access via terminal session.At the time the Reliability standards was approved the concept of supervised remote access was known. The Interpretation Drafting Team can only conclude that the original Standard Drafting Team did not list specific requirements for this type of access. The Interpretation Drafting Team cannot conclude that this type of access was prohibited. The fact that CIP-007 does not contain a specific unescorted cyber access provision is irrelevant. CIP-007 R5 requires technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Supervised access via Webex is not unauthorized system access. When terminal session access is utilized, the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | activity is tracked by the Company. R5 does not state all authorized user activity, the Interpretation drafting team is adding the word authorized in its response and is expanding the scope.This conclusion is more sensible for service vendors and SCADA system providers. The Interpretation Drafting Team's interpretation would require, as the requestor noted, large vendors (such as CISCO) to take every entities cyber training course and submit to multiple background checks. This would be compliance for compliance sake and not for security. The Interpretation should have stated that the names of authorized individuals are maintained on a list. These individuals are required to comply with CIP-004 R2 through R4. Supervisory Cyber Access via terminal session is not prohibited explicitly by the Standards and is therefore allowed. There are no additional Reliability requirements for such access beyond those described in Standards CIP-002 through CIP-009. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. -Considering the Standards Development Process is outside the scope of the "Guidelines for Interpretation Drafting Teams" that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ."** | | |
| Progress Energy | No | Progress Energy disagrees with this interpretation and believes the intent of the standard is to allow for supervised/escorted access for both physical and cyber access (whether remote cyber or onsite cyber access). Registered Entities should be able to allow vendors providing support temporary, indirect, and monitored access to in scope NERC CIP assets via remote terminal sessions (Live Mtg, Webex, etc) (just as escorted physical access is allowed) without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4. In addition, Registered Entities should be able to allow vendors providing onsite temporary support escorted cyber access without having to meet the training, risk assessment and access requirements specified on CIP-004 R2, R3 and R4.There are multiple NERC CIP support vendors that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard. This |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | includes process control vendors not just IT vendors. Honeywell, GE, ABB, Siemens, Babcock and Wilcox, Emerson, GTE, Wood Group are all DCS vendors/tuners that may need to provide escorted cyber access at Progress Energy and throughout the industry. Not allowing for escorted cyber access could have adverse impacts to BES Reliability since some of this work is needed not only during emergencies but also for ongoing maintenance. Long term service agreements are in place with these vendors that have warranty implications that require escorted cyber support for various process control systems. Many Registered Entities rely on these vendors/tuners to provide their expertise in support of continual operations for proprietary systems and do not employ resources with these specialized skill sets. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br>**-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.**<br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Waterfall Security Solutions | No? | Unidirectional remote screen view products using hardware-enforced unidirectional communications or "data diodes" can securely show remote, unauthorized personnel the contents of screens on Critical Cyber Assets which are inside of an ESP. The technology allows remote personnel to watch and advise as authorized individuals carry out cyber access to those CCAs without introducing any risk that the remote personnel can directly influence the monitored CCAs in any way. This mechanism addresses WECC's concern regarding being "excessively burdened by limiting access to timely support." Since unidirectional remote screen view technology prevents the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | unauthorized observer from carrying out any direct cyber access, the unidirectional technology should have been identified in the interpretation as a legitimate form of supervised remote access. |
| **Response: Without commenting on specific technology, this comment raises access control and information protection considerations that are both outside the scope of this interpretation.** | | |
| Salt River Project | No | As written we disagree with the IDT team's interpretation of CIP-004. We recognize CIP-004 does not include the concept of any words relating to "escorting" or "supervision" in the requirement language. However, the interpretation is not clearly defined and reaches the conclusion that escorted electronic access is prohibited because a formal electronic access escorting requirement is not defined. It appears this conclusion was based on the fact that CIP-006 clearly defines "escorted" or "supervised" physical access to cyber assets. We believe this type of assumption sets a bad precedent for future interpretations.Additionally we believe this interpretation won't allow emergent electronic access when needed. We believe there is little or no risk associated with allowing escorted access to a known contracted support vendor, when support is needed. In fact we believe prohibiting this type of access increases the risk level to the BES. |
| **Response: -The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**-Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Austin Energy | No | We believe NERC should acknowledge that "escorted" cyber access is legitimate. If one of our employees is monitoring the cyber activities of the escorted vendor, our |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | employee could terminate the session if the vendor began to take inappropriate actions. This is akin to the situation for escorted physical access. As long as the person is escorted, if s/he begins to take inappropriate action, the escort can take appropriate responsive action. |
| **Response: As written the Standards do not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements. Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Essential Power, LLC | No | In its interpretation the IDT has ignored the previous guidance provided by NERC & FERC in regards to this Standard, as discussed by WECC in its request for interpretation.In its request, WECC also points out the practical difficulties of implementing the IDTs interpretation. Large vendor organizations work across multiple industries that are subject to a wide range of regulatory compliance, and work with multiple entities within any one industry; thus it would be impractical for them to require their personnel to go through the lengthy process of a PRA, training, etc. for EACH entity it works with in ALL areas in order to obtain unescorted cyber access to the systems for which they provide support.Additionally, this interpretation would place an unnecessary and considerable burden on smaller entities that are resource constrained. For example, if an entity needs to bring a SCADA engineer onsite because they cannot grant them escorted/monitored cyber access to the system, then they may need to fly them in from a different part of the country in order to perform the work. This increases the cost of the work by up to three times, and creates considerable delays in accomplishing the work. This could result in longer down-times for equipment and potentially be cost prohibitive. These results could discourage entities from performing routine or timely maintenance in order to avoid lengthy down-times or higher costs, potentially impacting the reliability & security of the BES; this is the opposite effect of what we should be looking for in the application of a Reliability Standard.There are a number of ways in which monitored cyber access can be performed to ensure the security of CCAs, while at the same time allowing entities and their vendors the flexibility needed to perform their |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | functions in a timely, cost effective manner. The monitoring method(s) used should be clearly documented and consistently applied by the registered entity, and audited by the CEA; this would provide reasonable assurance that the entity is minimizing the security risks associated with the monitored access. |
| **Response: The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. With respect to contracted or vendor support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.**<br><br>**Also, the interpretation must meet the "Guidelines for Interpretation Drafting Teams" that specify that "[a]n interpretation may only clarify or interpret the requirements of an approved Reliability Standard, . . ." Modification of the standard to allow electronic access, even from a vendor, without satisfying the existing requirements in CIP-004 is outside the scope of an interpretation.** | | |
| Midwest ISO | No | MISO respectfully submits that the IDT's proposed Interpretation of the phrase "authorized access" is unsupported by the plain language of CIP-004. The phrase "authorized access," which is the subject of the Interpretation, does not appear in CIP-004. Instead, the Standard uses the phrase "authorized cyber or authorized unescorted physical access." MISO understands that the question posed by the requestor utilized the term "Authorized Access", but respectfully submits that the IDT should have provided clarification specifically regarding authorized cyber access and authorized unescorted cyber access, which clarification would have resulted in entities ability to more directly apply the interpretation to its compliance efforts under CIP-004-1, R2. Moreover, the IDT's explanation of "authorized access" merely refers back to the requirements associated with access without providing the requested clarification. As a result, MISO does not agree with the Interpretation as to the answer provided in response to Question 1. As to the proposed answers to Questions 2 and 3, MISO respectfully submits that, without the specific clarification requested under Question 1, the Interpretation's conclusions are not sufficiently supported by the text of CIP-004. |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: The IDT sought to clarify the meaning of the term "authorized access" as requested by WECC because the requirement addresses "authorized cyber or authorized unescorted physical access." The IDT clarifies that authorized access in context of cyber access does not contemplate a notion of supervision or escorting. The IDT noted in the interpretation that neither the glossary nor the standard provided a definition of that term, and the IDT sought to provide clarity on the term as requested by the request for interpretation.** | | |
| CRSI | No | The response to question 1 attempts to define authorized access. The definition, even if local to CIP-004, should be expanded to include an indication that authorized access indicates personnel with approval to access Critical Cyber Assets. The presence of a person's name on a maintained list could be in error and would not be an indication of authorized access. |
| **Response: The IDT is not equating "authorized access" with being on the list, it is just noting that being on the list indicates that the other steps for authorization pursuant to the requirements have been completed. The requirement language addresses "electronic access," and all electronic access must be authorized.** | | |
| MISO Standards Collaborators | | We do not believe the standard separates how to treat cyber and physical access for vendors with regard to supervision. The interpretation says that temporary vendors can have unescorted and unsupervised cyber access if they have training on such things as specific policies, access controls, and procedures as developed by each individual Registered Entity. Training alone will not prevent a vendor from doing something malicious. Supervised access would be allowed and preferable instead of giving unrelated training and providing unsupervised access. |
| **Response: The IDT believes that the relevant question to resolve is not whether an entity *can* supervise remote cyber access, but whether such access is allowed by the standard.** | | |
| Omaha Public Power District | | From NERC Comment form (Sorry we did not get it submitted on time) 1. The NERC Board of Trustees indicated that the interpretation process should not be used to address requests for a decision on "how" a reliability standard applies to a registered entity's particular facts and circumstances. Do you believe this request for an interpretation is asking for clarity on the meaning of a requirement or clarity on the |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| | | application of a requirement? 0 The request is asking for clarity on the meaning of a requirement. 1 The request is asking for clarity on the application of a requirement. Comments: N/A 2. The NERC Board of Trustees indicated that in deciding whether or not to approve a proposed interpretation, it will use a standard of strict construction and not seek to expand the reach of the standard to correct a perceived gap or deficiency in the standard. Do you believe this interpretation expands the reach of the standard? 1 The interpretation expands the reach of the standard. 0 The interpretation does not expand the reach of the standard. Comments: OPPD respectfully disagrees with the proposed interpretation provided by NERC in response to questions submitted by WECC. Utilizing standards that are not in direct relation to the question being proposed contains no true definition or answer. This type of response sets an unacceptable precedence of using different standards and requirements to justify an interpretation. 3. Do you agree with this interpretation? If not, please explain specifically what you disagree with. 0 Yes 1 No Comments: In Q2 of the request for interpretation, WECC requests information regarding training, risk assessment and access requirements in R2, R3 and R4 applying to vendors who are supervised. NERC's response recognizes that supervision for physical access must occur when an individual is not authorized, but CIP-004-1 Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access. Another example referenced was CIP-006-1, Requirement R1.6, which defines procedures for escorted access within a physical security perimeter for unauthorized personnel. Again, NERC's answer is not clearly defined and reaches a conclusion that escorted electronic access is not allowed because a formal electronic access escorting requirement is not defined as it is with the CIP-006 R1.6 physical requirement. This type of correlation sets a bad precedent for future interpretations from NERC or Regional Entity auditors. Additionally, OPPD does not believe the interpretation allows for emergent electronic access when needed. OPPD believes there is little to no risk associated with allowing escorted access to a known contracted support vendor. Additionally, by not allowing this type of access, OPPD feels the risk level to the BES, in terms of reliability, is indeed increased. |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| **Response: -In response to the concern regarding other standards as references, the IDT notes that the purpose language of CIP-004 states, "Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3." The SDT referenced the other standards to illustrate that the visitor control program existed for physical access, and the standards are silent from a cyber access perspective when discussing visitors.<br>-The requirement language addresses "electronic access," and all electronic access must be authorized. While the IDT agrees that Requirement R2 does not explicitly deny the concept of escorted supervision for individuals with electronic access, it does not include a provision for "escorted" cyber access. Thus, any electronic access, whether "escorted" or not, must be authorized pursuant to the CIP-004 requirements.<br>-The IDT notes Version 2 and beyond allow exception of the training and personnel risk assessment authorization requirements in specified circumstances, including emergency situations. Furthermore, with respect to contracted support, the IDT notes that nothing prevents an entity from performing authorization for electronic access pursuant to the CIP-004 requirements. In that manner, the interpretation does not increase risk to the BES.<br>-Considering the provisions for emergency and planned access the IDT does not believe this interpretation increases the risk level to the BES.** | | |
| Bonneville Power Administration | Yes | |
| Kansas City Power & Light | Yes | |
| ISO/RTO Standards Review Committee | Yes | |
| Imperial Irrigation District (IID) | Yes | |
| PacifiCorp | Yes | |
| Xcel Energy | Yes | |
| NIPSCO | Yes | |

| Organization | Yes or No | Question 3 Comment |
|---|---|---|
| American Transmission Company, LLC | Yes | |
| Minnesota Power | Yes | |
| Duke Energy | Yes | |
| Independent Electricity System Operator | Yes | |
| E.ON CLIMATE & RENEWABLES | Yes | |
| Northeast Power Coordinating Council | Yes | |
| Great River Energy | Negative | Please see the formal comments submitted by ACES Power Marketing. |
| Brazos Electric Power Cooperative, Inc. | Negative | Please see comments to be submitted by ACES Power Marketing. |
| FirstEnergy Solutions | Negative | Please see FirstEnergy's comments submitted through the formal comment period. |
| Occidental Chemical | Negative | See comments submitted from Ingelside Cogeneration LP |
| Omaha Public Power District | Negative | Please Doug Peterchuck's comments. |
| **Response: Thank you for your comments.** | | |

END OF REPORT

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

**Note: an Interpretation cannot be used to change a standard.**

| Request for an Interpretation of a Reliability Standard |
|---|
| Date submitted: 10/15/09 |
| Date accepted: 10/23/09 |
| **Contact information for person requesting the interpretation:** |
| Name: John Van Boxtel |
| Organization: Western Electricity Coordinating Council |
| Telephone: 360-713-9090 |
| E-mail: jvanboxtel@wecc.biz |
| **Identify the standard that needs clarification:** |
| Standard Number: CIP-004-1 |
| Standard Title: Cyber Security – Personnel and Training |
| **Identify specifically what requirement needs clarification:** |

**Requirement Number and Text of Requirement:** R2, R3, and R4

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

**Clarification needed (emphasis added):**

Specifically, the WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would

temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

**Background**

Through previously published documents, both NERC and FERC have indicated that the intent of the CIP-004 Standard was to document training, risk assessment, and access to Critical Cyber Assets in situations where personnel have direct and unmonitored access to critical cyber assets, as opposed to and distinguishable from **supervised access.**

The question asked in Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training is: "*What is meant by 'authorized cyber access?'" The answer provided is:*

> *The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.* (emphasis added)

This answer is also consistent with a similar description of escorted access provided in FERC Order 706, page 116, paragraph 432, in which the Commission stated:

> *Entergy and SDG&E recommend that newly-hired employees be allowed access to critical cyber assets if they are accompanied by qualified escorts. We note that a qualified escort would have to possess enough expertise regarding the critical cyber asset to ensure that the actions of the newly-hired employee or vendor did not harm the integrity of the critical cyber asset or the reliability of the Bulk-Power system. However, if the escort is sufficiently qualified, we believe such escorted access could be permitted before a newly-hired employee is trained.* (emphasis added)

**Identify the material impact associated with this interpretation:**

Identify the material impact to your organization or others caused by the lack of clarity or an incorrect interpretation of this standard.

**Material Impact**

If "Authorized Access" includes temporary support access provided in a supervised manner, then there is a potential for many Registered Entities to either be noncompliant while seeking support, or excessively burdened by limiting access to timely support. This situation is particularly likely from large non-utility vendors (such as Cisco Systems) that are either unable or unwilling to provide dedicated support personnel who have complied with each individual Registered Entity's specific cyber security training and risk assessment programs, as required by the standard.

Specifically the following requirements would create operational and administrative issues not only for Registered Entities but also for vendors in typical supervised support situations:

- Training covering the specific policies, access controls, and procedures as developed by each individual Registered Entity.
- A personnel risk assessment for all support personnel provided by each individual vendor, based on the cyber security training program developed by each individual Registered Entity.
- Timely updates to each Registered Entity's access list of all support personnel provided by each individual vendor, including changes in personnel at the vendor within the timeframes prescribed by the standard.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

## Project 2009-26: Response to Request for an Interpretation of NERC Standard CIP-004-1 for the Western Electricity Coordinating Council

The following interpretation of NERC Standard CIP-004-1 Cyber Security — Personnel & Training, Requirements R2, R3, and R4, was developed by the Cyber Security Order 706 SAR drafting team.

### Requirement Number and Text of Requirement

R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

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.

### Question

The WECC RC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

### Response

WECC asks three questions, which are listed below. The answer to each question follows the question.

1. WECC seeks clarification on the definition of "authorized access" as applied to temporary support from vendors.

   Answer: While the *Glossary of Terms used in NERC Reliability Standards* does not have a definition of "authorized access," CIP-004-1, Requirement R4 requires that an 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." For purposes of CIP-004-1, an individual has "authorized access" if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.

2. Do the training, risk assessment, and access requirements specified in R2, R3, and R4 apply to vendors who are supervised?

Answer: As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4.[1] Through the use of the qualifier "unescorted" with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions "escorted" or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to "physical access," the concept or any words relating to "escorting" or "supervision" in the requirement language is absent relative to cyber access.

3. Assuming that a "supervised" vendor is exempt from CIP-004-1, Requirements R2, R3, and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Answer: To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of "escorted" cyber access whatsoever in CIP-004, whether remotely or in person.

[1] The drafting team also notes that the FAQ referenced in the request for interpretation is not the same as an approved Reliability Standard and is not mandatory and enforceable. The FAQ was not developed or approved through the same standards development process, and cannot be used to substitute for the language in the standard itself. The drafting team also notes that the concept of unsupervised trusted access in the FAQ applies only to Version 1—which contained a 30 and 90 day provision for training and personnel risk assessments for personnel with authorized cyber access and authorized unescorted physical access—and it was not modified to conform to the changes made in subsequent versions.

## A. Introduction

**1. Title:** Cyber Security — Personnel & Training

**2. Number:** CIP-004-3

**3. Purpose:** Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

**4. Applicability:**

**4.1.** Within the text of Standard CIP-004-3, "Responsible Entity" shall mean:

**4.1.1** Reliability Coordinator.

**4.1.2** Balancing Authority.

**4.1.3** Interchange Authority.

**4.1.4** Transmission Service Provider.

**4.1.5** Transmission Owner.

**4.1.6** Transmission Operator.

**4.1.7** Generator Owner.

**4.1.8** Generator Operator.

**4.1.9** Load Serving Entity.

**4.1.10** NERC.

**4.1.11** Regional Entity.

**4.2.** The following are exempt from Standard CIP-004-3:

**4.2.1** Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

**4.2.2** Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

**4.2.3** Responsible Entities that, in compliance with Standard CIP-002-3, identify that they have no Critical Cyber Assets.

**5. Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

## B. Requirements

**R1.** Awareness — The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications (e.g., emails, memos, computer based training, etc.);
- Indirect communications (e.g., posters, intranet, brochures, etc.);
- Management support and reinforcement (e.g., presentations, meetings, etc.).

**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:

**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.

## C. Measures

**M1.** The Responsible Entity shall make available documentation of its security awareness and reinforcement program as specified in Requirement R1.

**M2.** The Responsible Entity shall make available documentation of its cyber security training program, review, and records as specified in Requirement R2.

**M3.** The Responsible Entity shall make available documentation of the personnel risk assessment program and that personnel risk assessments have been applied to all personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as specified in Requirement R3.

**M4.** The Responsible Entity shall make available documentation of the list(s), list review and update, and access revocation as needed as specified in Requirement R4.

## D. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority

**1.1.1** Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

**1.1.2** ERO for Regional Entity.

**1.1.3** Third-party monitor without vested interest in the outcome for NERC.

#### 1.2. Compliance Monitoring Period and Reset Time Frame

Not Applicable.

#### 1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

#### 1.4. Data Retention

**1.4.1** The Responsible Entity shall keep personnel risk assessment documents in accordance with federal, state, provincial, and local laws.

**1.4.2** The Responsible Entity shall keep all other documentation required by Standard CIP-004-3 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

**1.4.3** The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

#### 1.5. Additional Compliance Information

### 2. Violation Severity Levels (To be developed later.)

## E. Regional Variances

None identified.

### Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | 01/16/06 | D.2.2.4 — Insert the phrase "for cause" as intended. "One instance of personnel termination for cause…" | 03/24/06 |
| 1 | 06/01/06 | D.2.1.4 — Change "access control rights" to "access rights." | 06/05/06 |
| 2 | | Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.<br>Removal of reasonable business judgment.<br>Replaced the RRO with the RE as a responsible entity.<br>Rewording of Effective Date.<br>Reference to emergency situations.<br>Modification to R1 for the Responsible Entity to establish, document, implement, and maintain the awareness program.<br>Modification to R2 for the Responsible Entity to establish, document, implement, and maintain the training program; also stating the requirements for the cyber security training program.<br>Modification to R3 Personnel Risk Assessment to clarify that it pertains to personnel having authorized cyber or authorized unescorted physical access to "Critical Cyber Assets".<br>Removal of 90 day window to complete training and 30 day window to complete personnel risk assessments.<br>Changed compliance monitor to Compliance Enforcement Authority. | |
| 3 | | Update version number from -2 to -3 | |
| 3 | 12/16/09 | Approved by NERC Board of Trustees | Update |

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Recirculation Ballots Open

## April 20 – 30, 2012

### Project 2009-26 Interpretation of CIP-004-X for WECC

### Project 2010-INT-05 Interpretation of CIP-002-X for Duke

Recirculation ballot periods are now open through **8 p.m. Eastern on April 30, 2012**

**Now Available: Project 2009-26 | Project 2010-INT-05**

Recirculation ballots for the interpretation of CIP-004-X - Cyber Security – Personnel and Training for WECC and CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke are being conducted through **8 p.m. Eastern on April 30, 2012.**

The CIP-004-X Interpretation Drafting Team did not make any changes to the interpretation following the posting that ended on March 23, 2012.

The CIP-002-X Interpretation Drafting Team made a minor clarifying change in the Question 2 response by replacing the phrase, "without which" with the phrase "without the Cyber Asset" in the parenthetical as shown below:

- A Cyber Asset that "may" be used, but is not "required" (i.e., ~~without which~~ a Critical Asset cannot function as intended without the Cyber Asset) for the operation of a Critical Asset is not "essential to the operation of the Critical Asset" for purposes of Requirement R3.

A clean version of the interpretation for CIP-004-X has been posted on the project webpage and a clean and redline version of the interpretation for CIP-002-X has been posted on the project webpage.

### Instructions

In the recirculation ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the recirculation ballot window. If a ballot pool member does not participate in the recirculation ballot, that member's last vote cast in the previous ballot will be carried over.

## Next Steps

Voting results will be posted and announced after the ballot window closes. If approved, the interpretation(s) will be submitted to the Board of Trustees.

## Background

In May 2011, the Standards Committee appointed a standing CIP Interpretation Drafting Team and assigned the further development of all outstanding CIP Interpretations, including the two referenced in this announcement, to that team. Initial drafts of each of the two CIP Interpretations were developed by a drafting team consisting of a different group of members of the CIP Interpretation Drafting Team. Each team has reviewed all comments submitted in the previous posting of its interpretation, along with FERC orders issued since the previous posting, and responded to comments consistent with guidance adopted by the NERC Board of Trustees and the Standards Committee.

Information about the CIP Interpretation Drafting Team is available on the team's webpage, which contains links to each of the interpretations that the team is working on including the two being balloted now.

## Standards Development Process

The Standard Processes Manual contains all the procedures governing the standards development and interpretation processes. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica Benson at monica.benson@nerc.net.

*For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.*

North American Electric Reliability Corporation
3353 Peachtree Rd NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Standards Announcement

## Project 2009-26 Interpretation of CIP-004-X for WECC

## Project 2010-INT-05 Interpretation of CIP-002-X for Duke Energy

### Recirculation Ballot Results

Project 2009-26: Now Available
Project 2010-INT-05: Now Available

Recirculation ballots for the interpretation of CIP-004-X - Cyber Security – Personnel and Training for WECC and CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke both concluded April 30, 2012.

Voting statistics for the ballots are listed below, and the Ballot Results page provides a link to the detailed results.

| Standard | Quorum | Approval |
|---|---|---|
| CIP-004-X - Cyber Security – Personnel and Training for WECC | Quorum: 90.96% | Approval: 80.08% |
| CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke | Quorum: 92.68% | Approval: 94.61% |

**Next Steps**
CIP-004-X - Cyber Security – Personnel and Training for WECC and CIP-002-X - Cyber Security – Critical Cyber Asset Identification for Duke will be presented to the NERC Board of Trustees for adoption and subsequently filed with regulatory authorities.

**Background**
Additional information is available on the project pages.
Project 2009-26 and Project 2010-INT-05

**Standards Development Process**
The Standard Processes Manual contains all the procedures governing the standards development process. The success of the NERC standards development process depends on stakeholder participation. We extend our thanks to all those who participate. For more information or assistance, please contact Monica

Benson at monica.benson@nerc.net.

*For more information or assistance, please contact Monica Benson, Standards Process Administrator, at monica.benson@nerc.net or at 404-446-2560.*

## Ballot Results

| | |
|---|---|
| **Ballot Name:** | Project 2009-26 Recirculation Ballot April 2012 CIP-004-x |
| **Ballot Period:** | 4/20/2012 - 4/30/2012 |
| **Ballot Type:** | Initial |
| **Total # Votes:** | 302 |
| **Total Ballot Pool:** | 332 |
| **Quorum:** | **90.96 % The Quorum has been reached** |
| **Weighted Segment Vote:** | 80.08 % |
| **Ballot Results:** | **The Standard has passed.** |

## Summary of Ballot Results

| Segment | Ballot Pool | Segment Weight | Affirmative # Votes | Affirmative Fraction | Negative # Votes | Negative Fraction | Abstain # Votes | No Vote |
|---|---|---|---|---|---|---|---|---|
| 1 - Segment 1. | 85 | 1 | 58 | 0.784 | 16 | 0.216 | 7 | 4 |
| 2 - Segment 2. | 10 | 0.7 | 7 | 0.7 | 0 | 0 | 2 | 1 |
| 3 - Segment 3. | 78 | 1 | 50 | 0.735 | 18 | 0.265 | 2 | 8 |
| 4 - Segment 4. | 23 | 1 | 16 | 0.889 | 2 | 0.111 | 3 | 2 |
| 5 - Segment 5. | 74 | 1 | 39 | 0.684 | 18 | 0.316 | 8 | 9 |
| 6 - Segment 6. | 46 | 1 | 25 | 0.694 | 11 | 0.306 | 5 | 5 |
| 7 - Segment 7. | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 - Segment 8. | 8 | 0.7 | 6 | 0.6 | 1 | 0.1 | 1 | 0 |
| 9 - Segment 9. | 2 | 0.1 | 1 | 0.1 | 0 | 0 | 0 | 1 |
| 10 - Segment 10. | 6 | 0.6 | 5 | 0.5 | 1 | 0.1 | 0 | 0 |
| **Totals** | **332** | **7.1** | **207** | **5.686** | **67** | **1.414** | **28** | **30** |

## Individual Ballot Pool Results

| Segment | Organization | Member | Ballot | Comments |
|---|---|---|---|---|
| 1 | Ameren Services | Kirit Shah | Negative | View |
| 1 | American Electric Power | Paul B. Johnson | Affirmative | View |
| 1 | American Transmission Company, LLC | Andrew Z Pusztai | Affirmative | |
| 1 | Arizona Public Service Co. | Robert Smith | Affirmative | |
| 1 | Associated Electric Cooperative, Inc. | John Bussman | Affirmative | |
| 1 | Avista Corp. | Scott J Kinney | Affirmative | |
| 1 | Balancing Authority of Northern California | Kevin Smith | Affirmative | |
| 1 | Baltimore Gas & Electric Company | Gregory S Miller | Affirmative | View |

| | | | | |
|---|---|---|---|---|
| 1 | BC Hydro and Power Authority | Patricia Robertson | Abstain | |
| 1 | Beaches Energy Services | Joseph S Stonecipher | Affirmative | |
| 1 | Black Hills Corp | Eric Egge | Affirmative | |
| 1 | Bonneville Power Administration | Donald S. Watkins | Affirmative | View |
| 1 | Brazos Electric Power Cooperative, Inc. | Tony Kroskey | Negative | View |
| 1 | CenterPoint Energy Houston Electric, LLC | John Brockhan | Affirmative | |
| 1 | City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power | Chang G Choi | Affirmative | |
| 1 | Clark Public Utilities | Jack Stamper | Affirmative | |
| 1 | Colorado Springs Utilities | Paul Morland | Affirmative | |
| 1 | Consolidated Edison Co. of New York | Christopher L de Graffenried | Affirmative | View |
| 1 | Corporate Risk Solutions, Inc. | Joseph Doetzl | Affirmative | |
| 1 | CPS Energy | Richard Castrejana | Affirmative | |
| 1 | Dominion Virginia Power | Michael S Crowley | Negative | View |
| 1 | Duke Energy Carolina | Douglas E. Hils | Affirmative | |
| 1 | Entergy Services, Inc. | Edward J Davis | Negative | View |
| 1 | FirstEnergy Corp. | William J Smith | Negative | View |
| 1 | Florida Keys Electric Cooperative Assoc. | Dennis Minton | Affirmative | |
| 1 | Florida Power & Light Co. | Mike O'Neil | Negative | |
| 1 | FortisBC | Curtis Klashinsky | Affirmative | |
| 1 | Georgia Transmission Corporation | Jason Snodgrass | Affirmative | |
| 1 | Great River Energy | Gordon Pietsch | Negative | View |
| 1 | Hoosier Energy Rural Electric Cooperative, Inc. | Bob Solomon | Negative | |
| 1 | Hydro One Networks, Inc. | Ajay Garg | Affirmative | |
| 1 | Idaho Power Company | Ronald D. Schellberg | Affirmative | |
| 1 | Imperial Irrigation District | Tino Zaragoza | Affirmative | View |
| 1 | International Transmission Company Holdings Corp | Michael Moltane | Affirmative | |
| 1 | Kansas City Power & Light Co. | Michael Gammon | Affirmative | |
| 1 | Lakeland Electric | Larry E Watt | Affirmative | |
| 1 | Lincoln Electric System | Doug Bantam | Affirmative | |
| 1 | Long Island Power Authority | Robert Ganley | Affirmative | |
| 1 | Los Angeles Department of Water & Power | John Burnett | | |
| 1 | Lower Colorado River Authority | Martyn Turner | | |
| 1 | Manitoba Hydro | Joe D Petaski | Affirmative | |
| 1 | MEAG Power | Danny Dees | Affirmative | |
| 1 | MidAmerican Energy Co. | Terry Harbour | Negative | View |
| 1 | Minnesota Power, Inc. | Randi K. Nyholm | Affirmative | |
| 1 | Minnkota Power Coop. Inc. | Theresa Allard | Affirmative | |
| 1 | Nebraska Public Power District | Cole C Brodine | Affirmative | |
| 1 | New York Power Authority | Bruce Metruck | Affirmative | |
| 1 | Northeast Utilities | David Boguslawski | Affirmative | |
| 1 | Northern Indiana Public Service Co. | Kevin M Largura | Affirmative | |
| 1 | NorthWestern Energy | John Canavan | Abstain | |
| 1 | Ohio Valley Electric Corp. | Robert Mattey | Affirmative | |
| 1 | Oklahoma Gas and Electric Co. | Marvin E VanBebber | Abstain | |
| 1 | Omaha Public Power District | Doug Peterchuck | Negative | View |
| 1 | Oncor Electric Delivery | Jen Fiegel | Affirmative | |
| 1 | PacifiCorp | Ryan Millard | Affirmative | |
| 1 | PECO Energy | Ronald Schloendorn | Abstain | |
| 1 | Platte River Power Authority | John C. Collins | Affirmative | |
| 1 | Portland General Electric Co. | John T Walker | Affirmative | |
| 1 | Potomac Electric Power Co. | David Thorne | Affirmative | |
| 1 | PowerSouth Energy Cooperative | Larry D Avery | Affirmative | |
| 1 | PPL Electric Utilities Corp. | Brenda L Truhe | Affirmative | |
| 1 | Progress Energy Carolinas | Brett A Koelsch | Negative | View |
| 1 | Public Service Company of New Mexico | Laurie Williams | Affirmative | |
| 1 | Public Service Electric and Gas Co. | Kenneth D. Brown | Affirmative | |
| 1 | Puget Sound Energy, Inc. | Denise M Lietz | Abstain | |
| 1 | Rochester Gas and Electric Corp. | John C. Allen | Affirmative | |
| 1 | Sacramento Municipal Utility District | Tim Kelley | Affirmative | |
| 1 | Salt River Project | Robert Kondziolka | Negative | View |
| 1 | SCE&G | Henry Delk, Jr. | | |
| 1 | Seattle City Light | Pawel Krupa | Abstain | |
| 1 | Sierra Pacific Power Co. | Rich Salgo | Affirmative | |
| 1 | Snohomish County PUD No. 1 | Long T Duong | Affirmative | |
| 1 | South California Edison Company | Steven Mavis | Affirmative | |

| | | | | |
|---|---|---|---|---|
| 1 | Southern Company Services, Inc. | Robert A. Schaffeld | Negative | View |
| 1 | Southwest Transmission Cooperative, Inc. | James Jones | Negative | View |
| 1 | Sunflower Electric Power Corporation | Noman Lee Williams | Affirmative | |
| 1 | Tampa Electric Co. | Beth Young | Negative | |
| 1 | Tennessee Valley Authority | Larry Akens | | |
| 1 | Trans Bay Cable LLC | Steven Powell | Abstain | |
| 1 | Tri-State G & T Association, Inc. | Tracy Sliman | Affirmative | |
| 1 | Tucson Electric Power Co. | John Tolo | Affirmative | |
| 1 | United Illuminating Co. | Jonathan Appelbaum | Negative | |
| 1 | Westar Energy | Allen Klassen | Affirmative | |
| 1 | Western Area Power Administration | Brandy A Dunn | Affirmative | |
| 1 | Xcel Energy, Inc. | Gregory L Pieper | Affirmative | |
| 2 | Alberta Electric System Operator | Mark B Thompson | Abstain | View |
| 2 | BC Hydro | Venkataramakrishnan Vinnakota | Abstain | |
| 2 | California ISO | Rich Vine | Affirmative | View |
| 2 | Electric Reliability Council of Texas, Inc. | Charles B Manning | Affirmative | View |
| 2 | Independent Electricity System Operator | Barbara Constantinescu | Affirmative | |
| 2 | ISO New England, Inc. | Kathleen Goodman | Affirmative | |
| 2 | Midwest ISO, Inc. | Marie Knox | Affirmative | View |
| 2 | New Brunswick System Operator | Alden Briggs | Affirmative | |
| 2 | New York Independent System Operator | Gregory Campoli | Affirmative | |
| 2 | Southwest Power Pool, Inc. | Charles H. Yeung | | |
| 3 | AEP | Michael E Deloach | Affirmative | View |
| 3 | Alabama Power Company | Richard J. Mandes | Negative | View |
| 3 | Ameren Services | Mark Peters | Negative | |
| 3 | APS | Steven Norris | Affirmative | |
| 3 | Arkansas Electric Cooperative Corporation | Philip Huff | Affirmative | |
| 3 | Atlantic City Electric Company | NICOLE BUCKMAN | Affirmative | |
| 3 | BC Hydro and Power Authority | Pat G. Harrington | Abstain | |
| 3 | Bonneville Power Administration | Rebecca Berdahl | Affirmative | |
| 3 | Central Lincoln PUD | Steve Alexanderson | Negative | View |
| 3 | City of Austin dba Austin Energy | Andrew Gallo | Affirmative | |
| 3 | City of Clewiston | Lynne Mila | Affirmative | |
| 3 | City of Farmington | Linda R Jacobson | Affirmative | |
| 3 | City of Garland | Ronnie C Hoeinghaus | Negative | View |
| 3 | City of Green Cove Springs | Gregg R Griffin | Affirmative | |
| 3 | City of Redding | Bill Hughes | Affirmative | |
| 3 | Consolidated Edison Co. of New York | Peter T Yost | Affirmative | |
| 3 | Constellation Energy | CJ Ingersoll | Affirmative | |
| 3 | Consumers Energy | Richard Blumenstock | Negative | View |
| 3 | Cowlitz County PUD | Russell A Noble | Affirmative | View |
| 3 | CPS Energy | Jose Escamilla | Affirmative | |
| 3 | Dayton Power & Light Co. | Jeffrey Fuller | Affirmative | |
| 3 | Delmarva Power & Light Co. | Michael R. Mayer | Affirmative | |
| 3 | Detroit Edison Company | Kent Kujala | Affirmative | |
| 3 | Dominion Resources Services | Michael F. Gildea | Negative | View |
| 3 | Duke Energy Carolina | Henry Ernst-Jr | Affirmative | |
| 3 | Entergy | Joel T Plessinger | Negative | |
| 3 | FirstEnergy Energy Delivery | Stephan Kern | Negative | View |
| 3 | Flathead Electric Cooperative | John M Goroski | Affirmative | |
| 3 | Florida Municipal Power Agency | Joe McKinney | Affirmative | |
| 3 | Florida Power Corporation | Lee Schuster | Negative | View |
| 3 | Georgia Power Company | Danny Lindsey | Negative | View |
| 3 | Georgia Systems Operations Corporation | William N. Phinney | Affirmative | |
| 3 | Great River Energy | Brian Glover | Negative | View |
| 3 | Gulf Power Company | Paul C Caldwell | Negative | View |
| 3 | Hydro One Networks, Inc. | David Kiguel | Affirmative | |
| 3 | Imperial Irrigation District | Jesus S. Alcaraz | Affirmative | |
| 3 | JEA | Garry Baker | Affirmative | |
| 3 | Kansas City Power & Light Co. | Charles Locke | Affirmative | |
| 3 | Kissimmee Utility Authority | Gregory D Woessner | | |
| 3 | Lakeland Electric | Norman D Harryhill | Affirmative | |
| 3 | Lincoln Electric System | Jason Fortik | Affirmative | |
| 3 | Los Angeles Department of Water & Power | Daniel D Kurowski | | |
| 3 | Louisville Gas and Electric Co. | Charles A. Freibert | Affirmative | |
| 3 | Manitoba Hydro | Greg C. Parent | Affirmative | |

| | | | | |
|---|---|---|---|---|
| 3 | MidAmerican Energy Co. | Thomas C. Mielnik | Negative | |
| 3 | Mississippi Power | Jeff Franklin | Negative | View |
| 3 | Municipal Electric Authority of Georgia | Steven M. Jackson | Affirmative | |
| 3 | Nebraska Public Power District | Tony Eddleman | Affirmative | |
| 3 | New York Power Authority | David R Rivera | Affirmative | |
| 3 | Niagara Mohawk (National Grid Company) | Michael Schiavone | Affirmative | |
| 3 | Northern Indiana Public Service Co. | William SeDoris | Affirmative | |
| 3 | Omaha Public Power District | Blaine R. Dinwiddie | Negative | View |
| 3 | Orange and Rockland Utilities, Inc. | David Burke | Affirmative | |
| 3 | Orlando Utilities Commission | Ballard K Mutters | Affirmative | |
| 3 | Owensboro Municipal Utilities | Thomas T Lyons | Affirmative | |
| 3 | Pacific Gas and Electric Company | John H Hagen | Negative | View |
| 3 | PacifiCorp | Dan Zollner | Affirmative | |
| 3 | Platte River Power Authority | Terry L Baker | Affirmative | |
| 3 | PNM Resources | Michael Mertz | Affirmative | |
| 3 | Potomac Electric Power Co. | Robert Reuter | | |
| 3 | Progress Energy Carolinas | Sam Waters | | |
| 3 | Public Service Electric and Gas Co. | Jeffrey Mueller | Affirmative | |
| 3 | Public Utility District No. 1 of Benton County | Gloria Bender | Affirmative | |
| 3 | Public Utility District No. 1 of Clallam County | David Proebstel | Affirmative | |
| 3 | Puget Sound Energy, Inc. | Erin Apperson | | |
| 3 | Sacramento Municipal Utility District | James Leigh-Kendall | Affirmative | |
| 3 | Salt River Project | John T. Underhill | Negative | View |
| 3 | San Diego Gas & Electric | Scott Peterson | | |
| 3 | Seattle City Light | Dana Wheelock | Abstain | |
| 3 | Seminole Electric Cooperative, Inc. | James R Frauen | Affirmative | |
| 3 | Snohomish County PUD No. 1 | Mark Oens | Affirmative | |
| 3 | South Carolina Electric & Gas Co. | Hubert C Young | | |
| 3 | Tampa Electric Co. | Ronald L Donahey | Negative | |
| 3 | Tennessee Valley Authority | Ian S Grant | | |
| 3 | Tri-State G & T Association, Inc. | Janelle Marriott | Affirmative | |
| 3 | Westar Energy | Bo Jones | Affirmative | |
| 3 | Wisconsin Electric Power Marketing | James R Keller | Affirmative | |
| 3 | Xcel Energy, Inc. | Michael Ibold | Affirmative | |
| 4 | American Municipal Power | Kevin Koloini | Affirmative | |
| 4 | Blue Ridge Power Agency | Duane S Dahlquist | Abstain | |
| 4 | City of Austin dba Austin Energy | Reza Ebrahimian | Affirmative | |
| 4 | City of Clewiston | Kevin McCarthy | Affirmative | |
| 4 | City of Redding | Nicholas Zettel | Affirmative | |
| 4 | City Utilities of Springfield, Missouri | John Allen | Abstain | |
| 4 | Consumers Energy | David Frank Ronk | Negative | View |
| 4 | Cowlitz County PUD | Rick Syring | Affirmative | |
| 4 | Flathead Electric Cooperative | Russ Schneider | Affirmative | |
| 4 | Florida Municipal Power Agency | Frank Gaffney | Affirmative | |
| 4 | Fort Pierce Utilities Authority | Thomas Richards | | |
| 4 | Georgia System Operations Corporation | Guy Andrews | Affirmative | |
| 4 | Madison Gas and Electric Co. | Joseph DePoorter | Affirmative | View |
| 4 | Northern California Power Agency | Tracy R Bibb | | |
| 4 | Ohio Edison Company | Douglas Hohlbaugh | Negative | View |
| 4 | Old Dominion Electric Coop. | Mark Ringhausen | Affirmative | |
| 4 | Public Utility District No. 1 of Douglas County | Henry E. LuBean | Affirmative | |
| 4 | Public Utility District No. 1 of Snohomish County | John D Martinsen | Affirmative | |
| 4 | Sacramento Municipal Utility District | Mike Ramirez | Affirmative | |
| 4 | Seattle City Light | Hao Li | Abstain | |
| 4 | Seminole Electric Cooperative, Inc. | Steven R Wallace | Affirmative | |
| 4 | Tacoma Public Utilities | Keith Morisette | Affirmative | |
| 4 | Wisconsin Energy Corp. | Anthony Jankowski | Affirmative | View |
| 5 | AEP Service Corp. | Brock Ondayko | Affirmative | View |
| 5 | Amerenue | Sam Dwyer | Negative | |
| 5 | Arizona Public Service Co. | Edward Cambridge | Affirmative | |
| 5 | Avista Corp. | Edward F. Groce | Affirmative | |
| 5 | BC Hydro and Power Authority | Clement Ma | Abstain | |
| 5 | Bonneville Power Administration | Francis J. Halpin | Affirmative | View |
| 5 | Brazos Electric Power Cooperative, Inc. | Shari Heino | Negative | View |
| 5 | City and County of San Francisco | Daniel Mason | Negative | View |
| 5 | City of Austin dba Austin Energy | Jeanie Doty | Affirmative | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 5 | City of Redding | Paul Cummings | Affirmative | |
| 5 | City Water, Light & Power of Springfield | Steve Rose | | |
| 5 | Cleco Power | Stephanie Huffman | | |
| 5 | Colorado Springs Utilities | Jennifer Eckels | Affirmative | |
| 5 | Consolidated Edison Co. of New York | Wilket (Jack) Ng | Affirmative | |
| 5 | Constellation Power Source Generation, Inc. | Amir Y Hammad | | |
| 5 | Consumers Energy Company | David C Greyerbiehl | Negative | View |
| 5 | Cowlitz County PUD | Bob Essex | Affirmative | |
| 5 | Dairyland Power Coop. | Tommy Drea | Affirmative | |
| 5 | Detroit Edison Company | Christy Wicke | Affirmative | |
| 5 | Dominion Resources, Inc. | Mike Garton | Negative | View |
| 5 | Duke Energy | Dale Q Goodwine | Affirmative | |
| 5 | Edison Mission Marketing & Trading Inc. | Brenda J Frazer | Affirmative | |
| 5 | Electric Power Supply Association | John R Cashin | Abstain | |
| 5 | Energy Services, Inc. | Tracey Stubbs | Negative | View |
| 5 | Essential Power, LLC | Patrick Brown | Negative | View |
| 5 | Exelon Nuclear | Michael Korchynsky | Abstain | |
| 5 | FirstEnergy Solutions | Kenneth Dresner | Negative | View |
| 5 | Florida Municipal Power Agency | David Schumann | Affirmative | |
| 5 | Great River Energy | Preston L Walsh | | |
| 5 | Imperial Irrigation District | Marcela Y Caballero | Affirmative | |
| 5 | JEA | John J Babik | Affirmative | |
| 5 | Kansas City Power & Light Co. | Brett Holland | Affirmative | |
| 5 | Kissimmee Utility Authority | Mike Blough | Affirmative | |
| 5 | Lakeland Electric | James M Howard | Affirmative | |
| 5 | Liberty Electric Power LLC | Daniel Duff | Negative | |
| 5 | Lincoln Electric System | Dennis Florom | Affirmative | |
| 5 | Los Angeles Department of Water & Power | Kenneth Silver | | |
| 5 | Manitoba Hydro | S N Fernando | Affirmative | |
| 5 | Massachusetts Municipal Wholesale Electric Company | David Gordon | Abstain | |
| 5 | MEAG Power | Steven Grego | Affirmative | |
| 5 | MidAmerican Energy Co. | Christopher Schneider | Negative | |
| 5 | Muscatine Power & Water | Mike Avesing | Abstain | |
| 5 | Nebraska Public Power District | Don Schmit | Affirmative | |
| 5 | New York Power Authority | Wayne Sipperly | Affirmative | |
| 5 | NextEra Energy | Allen D Schriver | Negative | |
| 5 | Northern Indiana Public Service Co. | William O. Thompson | Affirmative | |
| 5 | Occidental Chemical | Michelle R DAntuono | Negative | View |
| 5 | Omaha Public Power District | Mahmood Z. Safi | Negative | View |
| 5 | PacifiCorp | Sandra L. Shaffer | Affirmative | |
| 5 | Platte River Power Authority | Roland Thiel | Affirmative | |
| 5 | Portland General Electric Co. | Gary L Tingley | Affirmative | |
| 5 | PPL Generation LLC | Annette M Bannon | Affirmative | |
| 5 | Progress Energy Carolinas | Wayne Lewis | Negative | View |
| 5 | PSEG Fossil LLC | Tim Kucey | Affirmative | |
| 5 | Public Utility District No. 1 of Douglas County | Curtis A Wilkins | Affirmative | |
| 5 | Public Utility District No. 1 of Lewis County | Steven Grega | Abstain | |
| 5 | Puget Sound Energy, Inc. | Tom Flynn | | |
| 5 | Sacramento Municipal Utility District | Bethany Hunter | Affirmative | |
| 5 | Salt River Project | William Alkema | Negative | View |
| 5 | Seattle City Light | Michael J. Haynes | Abstain | |
| 5 | Seminole Electric Cooperative, Inc. | Brenda K. Atkins | Affirmative | |
| 5 | Snohomish County PUD No. 1 | Sam Nietfeld | Affirmative | |
| 5 | South Carolina Electric & Gas Co. | Edward Magic | | |
| 5 | Southern California Edison Co. | Denise Yaffe | Affirmative | |
| 5 | Southern Company Generation | William D Shultz | Negative | View |
| 5 | Tacoma Power | Claire Lloyd | Affirmative | View |
| 5 | Tampa Electric Co. | RJames Rocha | Negative | |
| 5 | Tenaska, Inc. | Scott M. Helyer | Abstain | |
| 5 | Tennessee Valley Authority | David Thompson | | |
| 5 | Tri-State G & T Association, Inc. | Barry Ingold | | |
| 5 | U.S. Army Corps of Engineers | Melissa Kurtz | Negative | View |
| 5 | U.S. Bureau of Reclamation | Martin Bauer | Affirmative | |
| 5 | Westar Energy | Bryan Taggart | Affirmative | |
| 5 | Wisconsin Electric Power Co. | Linda Horn | Affirmative | |
| 6 | AEP Marketing | Edward P. Cox | Affirmative | View |
| | | | | |

| | | | | |
|---|---|---|---|---|
| 6 | Ameren Energy Marketing Co. | Jennifer Richardson | Negative | |
| 6 | APS | RANDY A YOUNG | Affirmative | |
| 6 | Bonneville Power Administration | Brenda S. Anderson | Affirmative | |
| 6 | City of Austin dba Austin Energy | Lisa L Martin | Affirmative | |
| 6 | City of Redding | Marvin Briggs | Affirmative | |
| 6 | Cleco Power LLC | Robert Hirchak | | |
| 6 | Consolidated Edison Co. of New York | Nickesha P Carrol | Affirmative | |
| 6 | Constellation Energy Commodities Group | Brenda L Powell | Affirmative | |
| 6 | Entergy Services, Inc. | Terri F Benoit | Negative | View |
| 6 | Exelon Power Team | Pulin Shah | Abstain | |
| 6 | FirstEnergy Solutions | Kevin Querry | Negative | View |
| 6 | Florida Municipal Power Agency | Richard L. Montgomery | Affirmative | |
| 6 | Florida Municipal Power Pool | Thomas Washburn | Affirmative | |
| 6 | Florida Power & Light Co. | Silvia P. Mitchell | Negative | |
| 6 | Great River Energy | Donna Stephenson | | |
| 6 | Imperial Irrigation District | Cathy Bretz | Affirmative | |
| 6 | Kansas City Power & Light Co. | Jessica L Klinghoffer | Affirmative | |
| 6 | Lakeland Electric | Paul Shipps | Negative | View |
| 6 | Lincoln Electric System | Eric Ruskamp | Affirmative | |
| 6 | Los Angeles Department of Water & Power | Brad Packer | | |
| 6 | Luminant Energy | Brad Jones | Abstain | |
| 6 | Manitoba Hydro | Daniel Prowse | Affirmative | View |
| 6 | MidAmerican Energy Co. | Dennis Kimm | Negative | |
| 6 | New York Power Authority | Saul Rojas | Affirmative | |
| 6 | Northern Indiana Public Service Co. | Joseph O'Brien | Affirmative | View |
| 6 | NRG Energy, Inc. | Alan Johnson | Abstain | |
| 6 | Omaha Public Power District | David Ried | Negative | View |
| 6 | PacifiCorp | Scott L Smith | Affirmative | |
| 6 | Platte River Power Authority | Carol Ballantine | Affirmative | |
| 6 | Powerex Corp. | Daniel W. O'Hearn | | |
| 6 | PPL EnergyPlus LLC | Mark A Heimbach | Affirmative | |
| 6 | Progress Energy | John T Sturgeon | Negative | View |
| 6 | PSEG Energy Resources & Trade LLC | Peter Dolan | Affirmative | |
| 6 | Public Utility District No. 1 of Chelan County | Hugh A. Owen | Abstain | |
| 6 | Sacramento Municipal Utility District | Diane Enderby | Affirmative | |
| 6 | Salt River Project | Steven J Hulet | Negative | |
| 6 | Seattle City Light | Dennis Sismaet | Abstain | |
| 6 | Seminole Electric Cooperative, Inc. | Trudy S. Novak | Affirmative | |
| 6 | Snohomish County PUD No. 1 | William T Moojen | Affirmative | |
| 6 | South California Edison Company | Lujuanna Medina | Affirmative | |
| 6 | Southern Company Generation and Energy Marketing | John J. Ciza | Negative | View |
| 6 | Tacoma Public Utilities | Michael C Hill | Affirmative | |
| 6 | Tampa Electric Co. | Benjamin F Smith II | Negative | |
| 6 | Tennessee Valley Authority | Marjorie S. Parsons | | |
| 6 | Westar Energy | Grant L Wilkerson | Affirmative | |
| 8 | | Roger C Zaklukiewicz | Affirmative | |
| 8 | | Edward C Stein | Affirmative | |
| 8 | | James A Maenner | Abstain | |
| 8 | APX | Michael Johnson | Affirmative | |
| 8 | JDRJC Associates | Jim Cyrulewski | Affirmative | |
| 8 | Massachusetts Attorney General | Frederick R Plett | Affirmative | |
| 8 | Network & Security Technologies | Nicholas Lauriat | Affirmative | |
| 8 | Volkmann Consulting, Inc. | Terry Volkmann | Negative | |
| 9 | California Energy Commission | William M Chamberlain | | |
| 9 | Commonwealth of Massachusetts Department of Public Utilities | Donald Nelson | Affirmative | |
| 10 | New York State Reliability Council | Alan Adamson | Affirmative | |
| 10 | Northeast Power Coordinating Council | Guy V. Zito | Affirmative | |
| 10 | ReliabilityFirst Corporation | Anthony E Jablonski | Affirmative | |
| 10 | Southwest Power Pool RE | Emily Pennel | Negative | View |
| 10 | Texas Reliability Entity, Inc. | Donald G Jones | Affirmative | |
| 10 | Western Electricity Coordinating Council | Steven L. Rueckert | Affirmative | |
| | | | | |

Legal and Privacy : 609.452.8060 voice : 609.452.9550 fax : 116-390 Village Boulevard : Princeton, NJ 08540-5721
*Washington Office:* 1120 G Street, N.W. : Suite 990 : Washington, DC 20005-3801

Account Log-In/Register

Copyright © 2010 by the North American Electric Reliability Corporation. : All rights reserved.
A New Jersey Nonprofit Corporation

## Exhibit E

Roster of the Interpretation Drafting Team for the interpretation of Requirements R2, R3, and R4 of CIP-004-4 — Personnel and Training.

| Name and Title | Company and Address | Contact Info | Bio |
|---|---|---|---|
| Tim Conway, Chair<br>Director, NERC Compliance and Operations Technology | NIPSCO<br>1500 165th ST<br>Hammond, IN | (219) 853-4202<br>tjconway@nisource.com | Mr. Conway is Director of NERC Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). Formerly, he was an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He is the former Chair of the RFC CIPC and current Co-Chair of the NERC CIP Interpretation Drafting Team. Mr. Conway holds an MBA from the University of Notre Dame, a BS in Electrical Engineering Technology from Purdue University, and he has the obtained following professional certifications throughout his career: RHCT, SANS GCIH, CNE, Network +, CCNA, CISA, CRISC. |
| David Blackburn<br>Senior Information Security Risk Analyst | California Independent System Operator Corporation<br>250 Outcropping Way<br>Folsom, CA 95630 | (916) 351-2210<br>dblackburn@caiso.com | David J Blackburn has over 20 years of diverse experience with increasing responsibilities in IT repair, database programming, automatic test equipment, logistics, office automation, workstation support, application support, server support, training and evangelism, network engineering and network, application and information security. Mr. Blackburn's current work includes operational security incident and event management duties and strategic input on CIP 004, 005 and 007 and NISTIR 7628, as well as corporate information security policy. Mr. Blackburn is active in the professional security communities (ISSA, ISC^2 and ISACA), regularly serving in volunteer positions. Mr. Blackburn has a Bachelor of Science in Electronics Engineering Technology, and holds CISA and CISSP certifications. |
| Marc Child<br>Information Security Program Manager | Great River Energy<br>12300 Elm Creek Blvd<br>Maple Grove, MN 55369 | (763)-445-5563<br>mchild@GREnergy.com | Marc Child is a CISSP and an information security professional with fifteen years experience in cyber, physical, personnel, and data security. As Cyber Security Program Manager for Great River Energy, he has responsibility for managing the design and implementation of a security program for Minnesota's second largest electric utility, including NERC CIP. Marc currently serves as a cyber security subject-matter expert on the Critical Infrastructure Protection Committee at NERC – and in various security roles with the Midwest Reliability Organization. |

| | | | |
|---|---|---|---|
| David Dunn<br>Manager, Organizational Governance Support, IESO | Ontario IESO<br>Box 4474<br>Toronto, Ontario, Canada M5W4E5 | (905)855-6286<br>david.dunn@ieso.ca | David Dunn has been actively engaged in the CIP Standards since 2008 he was a member of a NERC Standards Drafting Team Project on Cyber Security Violation Severity Levels. As part of that team he was involved in developing interpretations as well. Mr. Dunn works closely with his company's compliance arm performing TFE assessments for Ontario and providing subject matter expertise to any cyber-related compliance issues. He has several years of IT Audit experience and is past chair and current member of the ISO/RTO Council Security Working Group. He is also a member of the Energy Sector Cyber Security Working Group, which is sponsored by the DoE |
| Amanda Mullenix<br>Generation NERC Compliance | Duke Energy<br>1000 E Main St.,<br>Plainfield IN 46168 | (317) 838-2458<br>amanda.mullenix@duke-energy.com | Amanda has been part of Duke Energy's generation CIP compliance team for several years in varying capacities. More recently, she was selected to lead the CIP Access Management efforts as part of Duke's overall compliance program. In addition to the new role, Amanda continues to specialize in generation compliance and work on CIP version 4 implementation efforts. |
| Clayton Stooshnoff<br>Technical Analyst | FortisBC, Inc.<br>1290 Esplanade<br>Trail, BC, Canada V1R 4L4 | (250) 368-0359<br>clayton.stooshnoff@fortisbc.com | Clayton Stooshnoff graduated with honors from the Selkirk College Computer Information Systems (CIS) program in 2004 and was hired as a Technical Analyst with FortisBC in 2005. He began working on FortisBC's SCADA infrastructure and security in 2008 after receiving his SCADA security architect certification (CSSA). In 2009 he began working towards making FortisBC compliant with the NERC Critical Infrastructure Protection standards. As part of this process he has worked with many business units within FortisBC including: Generation, Transmission & Distribution, Network Operations, Information Systems, Project Management, Security, Communications, and Training. He has taken part in numerous Compliance User Group (CUG) meetings hosted by WECC, as well as Protecting Canada's Critical Infrastructure workshops hosted by the RCMP (Integrated Technological Crime Unit). He has recently become a member of the newly formed WICF CIP Standards and Compliance Strategies focus group consisting of various persons in the Western Electricity Coordinating Council region. |

| | | | |
|---|---|---|---|
| Laurent Webber<br>Reliability Compliance Program Manager | Western Area Power Administration<br>12155 West Alameda Parkway<br>Lakewood, CO 80228 | (720) 962-7216<br>webber@wapa.gov | Laurent Webber received a bachelor degree in Electronic Engineering in 1984 and has worked at Western Area Power Administration (Western) for 28 years. Mr. Webber began his career at Western in Communication Engineering and advanced to teaching Power System Operation at Western's Electric Power Training Center. In addition to teaching the concepts of electrical power system operation, control, and response Mr. Webber worked to design, implement, and maintain SCADA and Power Plant simulators, relay protection systems, and industrial controls. Mr. Webber has experience with the real time operation of the bulk power system, in particular the communications and energy management systems and tools typically used by reliability coordinators, transmission operators, and generator operators.<br>Mr. Webber accepted a position as Western's Cyber Security Program Manager in 1999, and late in 2010 was promoted to Western's Reliability Compliance Program Manager. His extensive experience in cyber security includes years of awareness and tracking of cyber security vulnerabilities, exploits, impacts, and analysis of cyber attacks on all types of systems including power systems controls. In addition to the technical aspects of cyber security, Mr. Webber is familiar with government, DOE, NIST, NERC, and industry standards for information security, and has participated in drafting related DOE and Western policies. He has in-depth experience with interpreting, implementing, balancing, maintaining, and operating cyber security policies, practices, tools, and procedures. Mr. Webber has been deeply involved with Western's Critical Infrastructure protection program since before the NERC Urgent Action 1200 and has remained heavily involved throughout the implementation of the NERC CIP Cyber Security Standards. |