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.