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: 02/06/09
Contact information for person requesting the interpretation:
Name: Daniel Marvin
Organization: PacifiCorp
Telephone: 503.813.5375
E-mail: daniel.marvin@pacificorp.com
Identify the standard that needs clarification:
Standard Number: CIP-005-1-4.2.2 and CIP-005-1-R1.3
Standard Title: CIP-005-1 --Cyber Security -- Electronic Security Perimeters
Identify specifically what needs clarification:

Request for an Interpretation of a Reliability Standard

Requirement Number and Text of Requirement: **CIP-005-1 4.2.2 and R1.3**

4.2. The following are exempt from Standard CIP-005:

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.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

Clarification needed:

4.2.2 indicates that the communication links between ESPs and the required supporting equipment are not in the scope of this standard. However, in R1.3, the endpoints of a communication link between ESPs are required to be treated as "access points".

Regarding 4.2.2:

- What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?
- Is the communication link physical or logical? Where does it begin and terminate?

Regarding R1.3:

- Please clarify what is meant by an “endpoint”? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?
- If “endpoint” is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an “access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?

Identify the material impact associated with this interpretation:

Request for an Interpretation of a Reliability Standard

The material impact is potential non-compliance with the standard as written.

Many utilities have multiple control centers with fail over features between the facilities, and the communication links protected by encryption mechanisms such as VPN. Requiring all VPN termination points to also be access points introduces the requirement for strong authentication at the access point, increases complexity in network access controls and thus heightens probabilities of unintended failures, and will negatively impact real-time fail over functionality between control centers.

In addition, PacifiCorp is concerned regarding potential conflict with the published answer to Question #15, in the CIP-002-009 FAQ, "*Encryption or other data integrity checking technologies can also ensure that data is not changed in transit...*"

The following industry entities have a shared interest with PacifiCorp in this clarification request:

- Idaho Power
- Puget Sound Energy
- Platte River Power Authority
- Eugene Water & Electric Board
- Seattle City Light
- Arizona Public Service
- Bonneville Power Administration
- TransAlta
- Xcelenergy