



AESO Reliability Standards Monthly Report

September 2009

CIP-005-1 - Electronic Security Perimeters

Purpose:

Request for Interpretation by PacifiCorp.

Standard:

The standard had an effective date of June 1, 2006.

Request and Interpretation:

Question 1: 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?

NERC response: In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.

Question 2: Is the communication link physical or logical? Where does it begin and terminate?

NERC response: The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.

Question 3: For R1.3 please clarify what is meant by an "endpoint"? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?

NERC response: The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.

Question 4: 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?

NERC response: In the case where the "endpoint" is defined as logical and is \geq layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

Applicability:

Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, RRO

Current Status:

The interpretation was posted for ballot until Sept. 08, 2009. The AESO cast an abstain ballot. The interpretation received negative votes with comments and will proceed to a recirculation ballot after the drafting team addresses them.

NERC Link:

[Electronic Security Perimeters - RFI](#)