



AESO Reliability Standards Monthly Report

November/December 2009

CIP-006-1 - Physical Security

Purpose:

Request for Interpretation by PacifiCorp.

Standard:

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

Request and Interpretation:

Question 1: If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption?

Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

NERC response: For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("sixwall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

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 is posted for recirculation ballot until Dec. 23, 2009.

NERC Link:

[Physical Security - RFI](#)