AESO Reliability Standards Monthly Report

February 2009

CIP-006-1a - Physical Security of Critical Cyber Assets

Purpose:

Request for Interpretation.

Standard:

The US Army Corps of Engineers requested an interpretation to clarify requirements for monitoring and logging physical access referenced in Requirement R4.

> **R4 Logging Physical Access** — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
>
> **R4.1 Computerized Logging** - Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
>
> **R4.2 Video Recording** - Electronic capture of video images of sufficient quality to determine identity.
>
> **R4.3 Manual Logging** - A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

Request and Interpretation:

Question 1 - For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?

> **NERC Interpretation:** No monitoring and logging of access are only required for ingress at this time.

Question 2 - Does the term, "time of access" mean logging when the person entered the facility or does it mean logging the entry/exit time and "length" of time the person had access to the critical asset?

> **NERC Interpretation:** The term "time of access" refers to the time an authorized individual enters the physical security perimeter.

Applicability:

Balancing Authorities, Reliability Coordinators, Load-Serving Entities

Current Status:

The recirculation ballot period for the interpretation ended on February 16 and the AESO cast an affirmative ballot. The interpretation received 99% approval.

NERC Link:

Physical Security of Critical Cyber Assets