

## Request for an Interpretation of a Reliability Standard

Date submitted: September 12, 2008

### Contact information for person requesting the interpretation:

Name: Karl Bryan

Organization: US Army Corps of Engineers

Telephone: 503-808-3894

E-mail: karl.a.bryan@usace.army.mil

### Identify the standard that needs clarification:

Standard Number: CIP-006-1a

Standard Title: Cyber Security — Physical Security of Critical Cyber Assets

### Identify specifically what needs clarification

#### Requirement Number and Text of Requirement:

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.

**Clarification needed:** For physical access control to cyber assets, does this include monitoring when an individual leaves the controlled access cyber area?

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?

### 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.

A correct interpretation is needed for entities to determine whether existing systems are fully compliant with this requirement to avoid penalties associated with noncompliance.