



# AESO Reliability Standards Monthly Report

September 2009

## CIP-006-1 – Physical Security of Critical Cyber Assets

### **Purpose:**

Request for Interpretation by Progress Energy.

### **Standard:**

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

### **Request:**

CIP-002-1 R3 defines Critical Cyber Assets as assets essential to the operation of Critical Asset and assets meeting one of the characteristics of R3.1, R3.2 or R3.3. It is unclear from the stated requirements the extent ESP wiring external to physical security perimeter must be protected within a six wall boundary. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

### **NERC Interpretation:**

Interpretation of CIP-006-1 Requirement R1.1: "...to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. Progress Energy requests an interpretation as to the applicability of CIP-006-1 R1 to the aspects of the wiring that comprises the ESP.

### **Revised Response:**

The definition of Cyber Asset in the NERC Glossary of Terms Used in Reliability Standards includes communication networks. Physical media (wiring) is a component of a communication network within an Electronic Security Perimeter, but the wiring itself is not a separate Cyber Asset.

The specific situation described by Progress Energy involves physically separate Critical Cyber Assets connected by wiring inside the Electronic Security Perimeter. Since the connective wiring is inside the Electronic Security Perimeter, Requirement R1.1 of CIP-006-1 applies. CIP-006-1 R1.1 also provides: "Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets." For wiring within the Electronic Security Perimeter that is external to a Physical Security Perimeter, the alternative measures may be physical or logical, on the condition that they provide effective security, i.e., equivalent to or better than a completely enclosed ("six-wall") 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 balloting until Oct. 12, 2009.

### **NERC Link:**

[Physical Security of Critical Cyber Assets - RFI](#)