NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets for Progress Energy

Request for Interpretation Received from Progress Energy on April 2, 2008:

Request:
Progress Energy requests a formal interpretation of CIP-006-1. R1.1.

In CIP_006-1, Requirement 1.1 states "Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter. 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."

In CIP-005-1, Requirement 1 states "Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

In CIP-002-1, Requirement 3 states "Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

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.

CIP-006-1 Cyber Security – Physical Security of Critical Cyber Assets
R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. 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.

The following revised interpretation of CIP-006-1 — Physical Security of Critical Cyber Assets Requirement R1.1 was developed by the ~~Cyber Security Order 706 SAR drafting team~~CIP Interpretation Drafting Team's Project 2008-10 Interpretation Drafting Team in response to industry comments received from the second initial ballot:

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.~~

CIP-006-1, Requirement R1.1 applies to "Cyber Assets," and the first test in determining whether it applies to wiring is to determine whether wiring is a "Cyber Asset."
The definition of "Cyber Asset" in the *NERC Glossary of Terms Used in Reliability Standards* includes "communication networks," but it does not explicitly include wiring or communication mediums in general. Since wiring is not included in the definition of "Cyber Asset," Requirement R1.1 of CIP-006-1 does not apply to wiring.

This interpretation is limited to whether Requirement R1.1 applies to a particular circumstance (e.g, "wiring"), which makes it distinct from the interpretation in CIP-006-3c, appendix 3. The interpretation in CIP-006-3c, appendix 3, only applies when a completely enclosed ("six-wall") border cannot be established for a "Cyber Asset" within an Electronic Security Perimeter (ESP).