

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 Requirement 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 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 on July 2, 2008:

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.*

Response: The definition of a Cyber Asset includes both the data and the communication network, including the wiring that comprises the physical media supporting the network. The intent is to protect the data transmitted over the network within the ESP. Accordingly, the data must be protected from tampering, either through physical protection of the wiring or alternative protective measures.