Standard Review - CIP-006
Physical Security of Critical Cyber Assets

Shon Austin
Senior Compliance Specialist
CIP-006-3 Overview

Purpose: “CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.”

1. Identify Electronic Security Perimeters (ESPs)
2. Physically locate cyber assets within ESPs
3. Define/build your Physical Security Perimeter (PSP)
   a) May have to move some cyber assets
   b) May have to deal with special cases
4. Control, Monitor, and Log access
Identify ESP(s) and physically locate cyber assets within
Define/build your Physical Security Perimeter

• “The Box” – Traditional 6-wall boundary
  – Controlled, logged, and monitored access
  – Deters unauthorized access
  – ESP must be enclosed within the box
  – **Compliance Application Notice 31:**
    *CEAs are to consider 96 square inches as the measurement for each maximum acceptable opening without physical protective measures in place*

• Something else – Alternative measures
One ESP in one PSP: Control, Monitor & Log

Guard

Alarm

Biometric

Keypad

Logo

Test/Maintain

Camera

Control Center Building

PSP

Esp.
When you can not have the ideal “Box”

• Physical
  – Conduit
  – Fully enclosed cable tray
  – Armored cabling

• What happens when you can not control physical access?
PSP: Logical/Alternative Measures

• Logical
  – Data encryption
  – Circuit monitoring
    ▪ Detect unauthorized access
    ▪ Physical tampering

• Technical Feasibility Exception (TFE) required
One ESP, Two PSPs in one facility
Two ESPs in Two Facilities
One ESP spanning two facilities

“Protect the gap”
Document in Physical Security Plan

• Develop process to control, monitor, and log access
• Develop process/procedures to test and maintain controls
• These processes and procedures are your Physical Security Plan
• Ensure Physical Security Plan is approved by Senior Manager or delegate