Access Control and CIP
Agenda

• Access Control Requirements
• Impact on Entities
• Risk Discussion
• Response Discussion
• Future pursuit
Let’s Talk CIP
The CIP You Know

- Bulk Electric System
- Critical Assets
- Critical Cyber Assets
- CCA’s Covered by CIP
- Other Cyber Assets Covered by CIP
The CIP You Thought You Knew

Bulk Electric System

Critical Assets

Critical Cyber Assets

CCA’s Covered by CIP

Sufficiency Reviews / CIP V4 Attachment 1

CIP V4 / V5 changes

Other Cyber Assets Covered by CIP

BES Definition Changes

RFI on “essential” / CIP V5 changes
The CIP You Don’t Know

- Bulk Electric System
- Critical Assets
- Critical Cyber Assets
- CCA’s Covered by CIP
- Other Cyber Assets Covered by CIP
Access Control Requirements
CIP-003 R5

Requirement language:
R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
Requirement language:

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
Access Control

CCA’s Covered by CIP

Electronic Security Perimeter
Critical Cyber Assets

Physical Security Perimeter
Critical Assets

Other Cyber Assets Covered by CIP

Bulk Electric System

Access Control
Access Control

- CIP-003 R5
- CIP-004 R4
- CIP-005 R1.5, R2

Requirement language:
R1.5.Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s)
CIP-003 R5
CIP-004 R4
CIP-005 R1.5, R2
CIP-006 R1 – R6 all

Requirement language:

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s)
Impact on Entities
Impact of Requirements

Assets
- Physical Protection
- Electronic Protection
- Lists of individual access

Information
- Physical Protection
- Electronic Protection
- Lists of individuals who control access

People
- Qualifications for access (PRA / Training)
- Approval for access
- Removal of access
Risk Discussion
### Risks

1 Million Dollars a day per day - per violation

<table>
<thead>
<tr>
<th>Violation Risk Factor</th>
<th>Lower Range Limits</th>
<th>Moderate Range Limits</th>
<th>High Range Limits</th>
<th>Severe Range Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>$1,000</td>
<td>$2,000</td>
<td>$3,000</td>
<td>$5,000</td>
</tr>
<tr>
<td>Medium</td>
<td>$2,000</td>
<td>$4,000</td>
<td>$6,000</td>
<td>$10,000</td>
</tr>
<tr>
<td>High</td>
<td>$4,000</td>
<td>$8,000</td>
<td>$12,000</td>
<td>$20,000</td>
</tr>
</tbody>
</table>

- Lower range limits: $1,000 - $3,000
- Moderate range limits: $2,000 - $7,500
- High range limits: $3,000 - $15,000
- Severe range limits: $5,000 - $25,000

- Medium range limits: $2,000 - $100,000
- High range limits: $6,000 - $200,000
- Severe range limits: $10,000 - $335,000

- High range limits: $4,000 - $300,000
- High range limits: $8,000 - $625,000
- High range limits: $12,000 - $1,000,000
Risks

Previous 12 Months Violations Through August 31, 2011

Standards with Access Control Requirements
Risks

Everything is an island
Response Discussion
Response

Everything is an island

Build Bridges
Response

Risk Control - 2011 Project

Goals

Reduce Compliance Risk

Increase Situational Awareness

Active Policy Enforcement
# Response

<table>
<thead>
<tr>
<th>Reduce Compliance Risk</th>
<th>Increase Situational Awareness</th>
<th>Active Policy Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unique Id</td>
<td>• Employee actions</td>
<td>• Trigger Notification</td>
</tr>
<tr>
<td>• Simplify quarterly review</td>
<td>• Training records</td>
<td>• Disable physical access</td>
</tr>
<tr>
<td>• Reduce human performance errors</td>
<td>• PRA records</td>
<td>• Disable cyber access</td>
</tr>
<tr>
<td></td>
<td>• Reporting</td>
<td></td>
</tr>
</tbody>
</table>
Future Pursuits
Future

- Control Center Implementation
  - Increased awareness of events
    - Operator authentication
    - Operator multiple physical locations
    - Operator log on duration
  - Increased inputs to include system events and awareness data feeds
Future

- Field Implementations
  - Substation environments
  - Gen station environments

- Non-CIP
  - FERC regulations
  - Natural Gas facilities
Future

Everything is an island
Future
Questions