Supporting our customers with NERC CIP compliance

James McQuiggan, CISSP
Siemens Energy Sector

Energy products and solutions - in 6 Divisions

Enterprise Wide Power Generation Management

- Waste-fired Cogeneration Plants
- Coal-fired Power Plants
- Combined Cycle Plants
- Desalination Plants
- Coal Gasification Plants
- Wind Power Plants
- Nuclear Power Plants
- Industrial Power Plants
- Biomass Power Plants
- District Heat Power Plants

Mapping the CIP Standards to Siemens competencies

CIP Version 1 Current Standards

- CIP 001 – Sabotage Reporting
- CIP 002 – CCA Identification
- CIP 003 – Security Management
- CIP 004 – Personnel, Training
- CIP 005 – Electronic Security
- CIP 006 – Physical Security
- CIP 007 – Systems Security
- CIP 008 – Incident Reporting & Response
- CIP 009 – Recovery Plans

Siemens Capabilities to the NERC CIP Standards

- Siemens CERT – Cyber asset security and expertise (003, 005, 007)
- Global Data Pool – international personnel tracking and notification (004)
- Learn@ Siemens – NERC CIP CBT (004)
- Relationship with Verifications Inc (004)
- Information Security Program (004)
- Physical Security Expertise through Siemens Industry – Building Technologies Division (006)
- Expert I&C controls / Support (005, 007, 009)
- Member NERC Standards Committee (all)
- Security Consulting Services (all)
- CISSP, CPP Coordination (all)
Siemens NERC CIP Policies

- NERC CIP Compliance Database
  - Customer Notifications
    - 12 hours of termination
    - 7 days for other changes
  - Track employees training and background checks

- Siemens Critical Cyber Asset Training Program
  - Specific for CCA’s or BES cyber systems
  - Remote Access policies and procedures from Siemens (cRSP)
Siemens NERC CIP Policies

- Personal Risk Assessments
- 3rd party background check company

- Security Awareness Program

- Secure web-based screening
- ISO 9001:2000 certified
- Local and state for all 50 states

- Bi-annual manager and employee online training
- New-hire orientation program
- Information security advisor program
- Company Newsletters
- Internal control system – audits on information security
### NERC CIP Cyber Security Standards

#### CIP002-009 - Eight Standards / 41 Requirements

<table>
<thead>
<tr>
<th>CIP-002</th>
<th>CIP-003</th>
<th>CIP-004</th>
<th>CIP-005</th>
<th>CIP-006</th>
<th>CIP-007</th>
<th>CIP-008</th>
<th>CIP-009</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL CYBER ASSETS</td>
<td>SECURITY MANAGEMENT CONTROLS</td>
<td>PERSONNEL AND TRAINING</td>
<td>ELECTRONIC SECURITY</td>
<td>PHYSICAL SECURITY</td>
<td>SYSTEMS SECURITY MANAGEMENT</td>
<td>INCIDENT REPORTING &amp; RESPONSE PLANNING</td>
<td>RECOVERY PLANS FOR CCA</td>
</tr>
<tr>
<td>1. CRITICAL ASSETS</td>
<td>1. SECURITY POLICY</td>
<td>1. AWARENESS</td>
<td>1. ELECTRONIC SECURITY PERIMETER</td>
<td>1. PLAN</td>
<td>1. TEST PROCEDURES</td>
<td>1. RECOVERY PLANS</td>
<td>BLACK – Customer Responsibility</td>
</tr>
<tr>
<td>2. CRITICAL CYBER ASSETS</td>
<td>2. LEADERSHIP</td>
<td>2. TRAINING</td>
<td>2. ELECTRONIC ACCESS CONTROLS</td>
<td>2. PHYSICAL ACCESS CONTROLS</td>
<td>2. EXERCISES</td>
<td>RED – T3000 Feature</td>
<td></td>
</tr>
<tr>
<td>3. ANNUAL REVIEW</td>
<td>3. EXCEPTIONS</td>
<td>3. PERSONNEL RISK ASSESSMENT</td>
<td>3. MONITORING ELECTRONIC ACCESS</td>
<td>3. SECURITY PATCH MANAGEMENT</td>
<td>3. CHANGE CONTROL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. ANNUAL APPROVAL</td>
<td>4. INFORMATION PROTECTION</td>
<td>4. ACCESS</td>
<td>4. CYBER VULNERABILITY ASSESSMENT</td>
<td>4. MALICIOUS SOFTWARE PREVENTION</td>
<td>4. BACKUP &amp; RESTORE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. ACCESS CONTROL</td>
<td></td>
<td>5. DOCUMENTATION</td>
<td>5. ACCOUNT MANAGEMENT</td>
<td>5. TESTING BACKUP MEDIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. CHANGE CONTROL</td>
<td></td>
<td>Siemens Building Technology (SBT)</td>
<td>6. SECURITY STATUS MONITORING</td>
<td>BLUE – Siemens Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additional Information:**
- **CRITICAL ASSETS**
- **CRITICAL CYBER ASSETS**
- **ANNUAL REVIEW**
- **ANNUAL APPROVAL**
- **ELECTRONIC SECURITY PERIMETER**
- **ELECTRONIC ACCESS CONTROLS**
- **MONITORING ELECTRONIC ACCESS**
- **CYBER VULNERABILITY ASSESSMENT**
- **DOCUMENTATION**
SPPA-T3000 Control System Security Features

- SPPA-T3000 ESP and security zone architecture (Defense in Depth)
- Secure remote access
- Monitoring
- Malware protection software
- Account management
- Security patch management
Getting Security “Baked-in”

- Work with your vendors to have the security baked in the products
  - They want to make “you” reliable AND secure
  - Flexibility, documentation and agreements (contracts)

- DHS Procurement Language
  - Helpful to assisting you with getting secure & reliable product
  - Discuss the OEM / Vendor security policies

- Develop a policy for vendors, 3rd party companies
  - Personal Risk Assessments
  - Training of their products
Questions ?