How we support our customers with NERC CIP

James McQuiggan, CISSP
Disclaimer

The information from this presentation is provided for informational purposes only. An customers adherence to the examples contained within this presentation does not constitute compliance with the NERC Compliance Monitoring and Enforcement Program ("CMEP") requirements, NERC Critical Infrastructure Protection ("CIP") Reliability Standards, or any other NERC Reliability Standards or rules. While the information included in this material may provide some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this material should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this presentation, to determine compliance with the CIP Reliability Standards.
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


Energy 3
McQuiggan / Vylkov
# NERC CIP Cyber Security Standards

## CIP-002 - Critical Assets
1. Critical Assets
2. Critical Cyber Assets
3. Annual Review
4. Annual Approval

## CIP-003 - Security Management Controls
1. Cyber Security Policy
2. Leadership
3. Exceptions
4. Information Protection
5. Access Control
6. Change Control

## CIP-004 - Personnel and Training
1. Awareness
2. Training
3. Personnel Risk Assessment
4. Access

## CIP-005 - Electronic Security
1. Electronic Security Perimeter
2. Electronic Access Controls
3. Monitoring Electronic Access
4. Cyber Vulnerability Assessment
5. Documentation

## CIP-006 - Physical Security
1. Plan
2. Physical Access Controls
3. Monitoring Physical Access
4. Logging Physical Access
5. Access Log Retention
6. Maintenance & Testing

## CIP-007 - Systems Security Management
1. Test Procedures
2. Ports & Services
3. Security Patch Management
4. Malicious Software Prevention
5. Account Management
6. Security Status Monitoring
7. Disposal or Redeployment
8. Cyber Vulnerability Assessment
9. Documentation

## CIP-008 - Incident Reporting & Response Planning
1. Cyber Security Incident Response Plan
2. Documentation

## CIP-009 - Recovery Plans for CCA
1. Recovery Plans
2. Exercises
3. Change Control
4. Backup & Restore
5. Testing Backup Media

---

**Black – Customer Responsibility**
**Red – T3000 Feature**
**Blue – Siemens Service**
**CIP 003: Security Management Controls**

SPPA-T3000 (Version 4.2) has been designed with the capability to meet applicable CIP 003 requirements

<table>
<thead>
<tr>
<th>NERC Req.</th>
<th>NERC Comment</th>
<th>Siemens Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Cyber Security Policy</td>
<td></td>
</tr>
<tr>
<td>R2</td>
<td>Leadership</td>
<td></td>
</tr>
<tr>
<td>R3</td>
<td>Exceptions</td>
<td>SPPA-T3000 Documentation</td>
</tr>
<tr>
<td>R4</td>
<td>Information Protection</td>
<td>Siemens Processes and Procedures</td>
</tr>
<tr>
<td>R5</td>
<td>Access Control</td>
<td>Siemens Processes and Procedures</td>
</tr>
<tr>
<td>R6</td>
<td>Change Control and Configuration Management</td>
<td>SPPA-T3000 Change Control and Configuration Management</td>
</tr>
</tbody>
</table>
## Siemens Approach to CIP 004 Requirements

<table>
<thead>
<tr>
<th>NERC Req.</th>
<th>NERC Comment</th>
<th>Siemens Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Awareness</td>
<td>Siemens Processes and Procedures</td>
</tr>
<tr>
<td>R2</td>
<td>Training</td>
<td>Siemens Processes and Procedures</td>
</tr>
<tr>
<td>R3</td>
<td>Personnel Risk Assessment</td>
<td>Siemens Processes and Procedures</td>
</tr>
<tr>
<td>R4</td>
<td>Access</td>
<td>Siemens Processes and Procedures</td>
</tr>
</tbody>
</table>
Siemens NERC Policies

- Security Awareness Program
- Verifications
  - Secure web-based screening
  - ISO 9001:2000 certified
  - Local and state for all 50 states
- Siemens Critical Cyber Asset Training Program
- Customer Notifications – Notification within 24 hours of employee termination (policy in development)

- Bi-annual manager and employee online training
- New-hire orientation program
- Information security advisor program
- EnergyLine newsletter security articles/ reminders
- Internal control system – audits on information security
NERC CIP Security Training

- Siemens Security Awareness Program

- For all Siemens employees with cyber or unescorted physical access to customer’s Critical Cyber Assets

- Product training is provided for personnel utilizing T3000, TXP, or other Critical Cyber Assets at customer’s plant

- Physical access might require additional customer training at site

Specific NERC CIP training program for CIP 004 Requirement 2
Siemens Personal Risk Assessments (PRA)

- Establish a database to track the completed PRAs respective to customer sites.
- Process and procedures for:
  - Background checks
  - State / Federal / Criminal
  - Customer notification of changes to access lists:
    - Physical
    - Cyber
SPPA-T3000 (Version 4.2) has been designed with the capability to meet applicable CIP 005 requirements.

<table>
<thead>
<tr>
<th>NERC Req.</th>
<th>NERC Comment</th>
<th>Siemens Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Electronic Security Perimeter</td>
<td>Security zone architecture of SPPA-T3000</td>
</tr>
<tr>
<td>R2</td>
<td>Electronic Access Controls</td>
<td>SPPA-T3000 Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SPPA-T3000 Secure remote access</td>
</tr>
<tr>
<td>R3</td>
<td>Monitoring Electronic Access</td>
<td>SPPA-T3000 Monitoring</td>
</tr>
<tr>
<td>R4</td>
<td>Cyber Vulnerability Assessment</td>
<td>Siemens consulting services</td>
</tr>
<tr>
<td>R5</td>
<td>Documentation Review and Maintenance</td>
<td>SPPA-T3000 Documentation &amp; Follow-up Long Term Support</td>
</tr>
</tbody>
</table>
SPPA-T3000 Secure Network Architecture
Siemens Remote Access (cRSP)

- common Remote Service Platform
  - Only on Siemens network
- Authorized users only
  - 2 Factor Authentication (PKI)
  - Grants
    - specific sites & application
  - Logging / Auditing
    - monthly reports / site
- Automatic Customer Notification

Siemens provides a remote solution for non-repudiation
<table>
<thead>
<tr>
<th>NERC Req.</th>
<th>NERC Comment</th>
<th>Siemens Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Test Procedures</td>
<td>ESP and Security zone architecture: SPPA-T3000 components are subject to security tests; non-SPPA-T3000 components are located outside of the ESP</td>
</tr>
<tr>
<td>R2</td>
<td>Ports and Services</td>
<td>SPPA-T3000 Hardening</td>
</tr>
<tr>
<td>R3</td>
<td>Security Patch Management</td>
<td>SPPA-T3000 Security patch management</td>
</tr>
<tr>
<td>R4</td>
<td>Malicious Software Prevention</td>
<td>SPPA-T3000 Malware protection software</td>
</tr>
<tr>
<td>R5</td>
<td>Account Management</td>
<td>SPPA-T3000 Monitoring and Account management</td>
</tr>
<tr>
<td>R6</td>
<td>Security Status Monitoring</td>
<td>SPPA-T3000 Monitoring</td>
</tr>
<tr>
<td>R7</td>
<td>Disposal or Redeployment</td>
<td>Siemens field service</td>
</tr>
<tr>
<td>R8</td>
<td>Cyber Vulnerability Assessment</td>
<td>Siemens consulting services</td>
</tr>
<tr>
<td>R9</td>
<td>Documentation Review and Maintenance</td>
<td>Siemens consulting services</td>
</tr>
</tbody>
</table>
### SPPA-T3000 (Version 4.2) CIP 009 Capabilities

<table>
<thead>
<tr>
<th>NERC Req.</th>
<th>NERC Comment</th>
<th>Siemens Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Recovery Plans</td>
<td>SPPA-T3000 Emergency plan</td>
</tr>
<tr>
<td>R2</td>
<td>Exercises</td>
<td>Siemens training service</td>
</tr>
<tr>
<td>R3</td>
<td>Change Control</td>
<td>Siemens consulting service</td>
</tr>
<tr>
<td>R4</td>
<td>Backup and Restore</td>
<td>SPPA-T3000 Emergency plan</td>
</tr>
<tr>
<td>R5</td>
<td>Testing Backup Media</td>
<td>Siemens field service</td>
</tr>
</tbody>
</table>
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 Contacts

- Siemens Customer – contact your Sales / Service Account Manager
- If you want to be a Siemens customer  [www.siemens.com/energy](http://www.siemens.com/energy)
- Siemens NERC CIP Questions:
  - James McQuiggan ([james.mcquiggan@siemens.com](mailto:james.mcquiggan@siemens.com))
  - Vladimir Vylkov ([vladimir.vylkov@siemens.com](mailto:vladimir.vylkov@siemens.com))
Thank you !