Security Regulations and Standards for SCADA and Industrial Controls

Overview of NERC CIP and other Security Frameworks
Topics Covered

• Mapping of US Government Agency Oversight to each Critical Infrastructure Sector

• Provide a current status of various SCADA Security references for adaptation by International markets

• NERC CIP, ISA SP99, CFATS, API 1164, NIST 800-82, NIST 800-53 rev3, AGA 12, CSSP DHS Best Practice Guides, etc...

• Use NERC CIP as a sample security framework, and break down the compliance requirements

• Actual security Incidents involving SCADA and Industrial Control Systems
Sources

- www.dhs.gov/nipp
- Meetings with DHS
- Meetings with NERC / FERC
- NERC CIP Consulting and CFATS Compliance Projects
- NERC CIP Standards (CIP-002 through CIP-009) [Link](http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html)
- NERC Cyber Security Standards Education Workshop (Workbook provided at training workshops)
- ISO / IEC 17799 and 270001
- ISA SP99 Volunteer Draft Development & Review
- Experience with over 100 assessments of Critical Infrastructure facilities over past seven years
What is the NIPP

• DHS was commissioned under the Homeland Security act of 2002 to develop one single approach or plan for protecting all 17 critical infrastructure sectors

• DHS developed the National Infrastructure Protection Plan (NIPP) to unify what was previously done in multiple various agencies to reduce redundancy and focus on one centralized approach.
• NIPP Mission

• Build a safer, more secure, and resilient America by enhancing protection of the Nation’s CI/KR (Critical Infrastructures / Key Resources) to prevent, deter, neutralize, or mitigate the effects of deliberate by terrorists to destroy, incapacitate, or exploit them, and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency
Map GOV Agencies to each CI Sector

<table>
<thead>
<tr>
<th>Sector-Specific Agency</th>
<th>Critical Infrastructure/Key Resources Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Agriculture&lt;sup&gt;1&lt;/sup&gt;</td>
<td>Agriculture and Food</td>
</tr>
<tr>
<td>Department of Health and Human Services&lt;sup&gt;2&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>Department of Defense&lt;sup&gt;3&lt;/sup&gt;</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Energy&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>Department of Health and Human Services</td>
<td>Public Health and Healthcare</td>
</tr>
<tr>
<td>Department of the Interior</td>
<td>National Monuments and Icons</td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Banking and Finance</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Drinking Water and Water Treatment Systems</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td>Chemical</td>
</tr>
<tr>
<td>Office of Infrastructure Protection</td>
<td>Commercial Facilities Dams</td>
</tr>
<tr>
<td></td>
<td>Emergency Services</td>
</tr>
<tr>
<td></td>
<td>Commercial Nuclear Reactors, Materials, and Waste</td>
</tr>
<tr>
<td>Office of Cyber Security and Telecommunications</td>
<td>Information Technology Telecommunications</td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td>Postal and Shipping</td>
</tr>
<tr>
<td>Transportation Security Administration,</td>
<td></td>
</tr>
<tr>
<td>United States Coast Guard&lt;sup&gt;5&lt;/sup&gt;</td>
<td>Transportation Systems&lt;sup&gt;6&lt;/sup&gt;</td>
</tr>
<tr>
<td>Immigration and Customs Enforcement,</td>
<td>Government Facilities</td>
</tr>
<tr>
<td>Federal Protective Service</td>
<td></td>
</tr>
</tbody>
</table>
Example: Energy Sector

- Energy Policy Act of 2005 (EPACT) called for the office and function of an ERO (Energy Reliability Organization) to develop and enforce a set of minimum physical and cyber security standards for the Bulk Electric System (BEP)

- FERC recognized NERC as the ERO in June 2006, and granted the right to levy financial fines and penalties for non-compliance

- NERC CIP standards become law in Jan 2007, and mandatory compliance begins in 2009 with financial penalties and audits beginning in 2010.

- Up to $1,000,000 per day per occurrence for non-compliance.

- Energy companies maintain all compliance proof at their facilities, do not submit anything to NERC. Compliance is audited by NERC going to utilities offices.
Security Standards end up being Regulated by Government when industry can not be accountable to be “Self Regulated”

"You should check your e-mails more often. I fired you over three weeks ago."
Example: Chemicals Sector

- DHS has direct authority over the Chemical sector and developed the CFATS (Chemical Facilities Anti-Terrorism Standards) to ensure that any organizations that manufacture, store, or transport hazardous chemicals have a baseline or minimum physical and cyber security measures in place.

- CFATS has specific steps and timeline for compliance

- DHS has the right to audit for non-compliance at any time, and can send agents into the facilities

- Non-compliance can result in “Cease to Operate” action taken by DHS to shut down the chemical operations

- Chemical organizations must submit documentation and inventories to a central DHS application called Top Screen
Government / Military Sectors: NIST 800-53

- All Federal systems must pass accreditation and certification processes based on NIST 800-53
- Control Systems and SCADA Systems in use at Federal installations could not pass certification testing due to their unique differences
- NIST 800-82 written as a best practice guide for securing SCADA systems
- NIST 800-53 updated to NIST 800-53a and SCADA specific language added. The current standard is NIST 800-53 rev3.
- The underlying technical systems cannot be commissioned and put into operational use if they are not compliant – no current financial penalties for non-compliance
<table>
<thead>
<tr>
<th>Sector-Specific Agency</th>
<th>Critical Infrastructure/Key Resources Sector</th>
<th>Security Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Agriculture</td>
<td>Agriculture and Food</td>
<td>TBD</td>
</tr>
<tr>
<td>Department of Health and Human Services</td>
<td></td>
<td>FIPS, FISMA, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Department of Defense</td>
<td>Defense Industrial Base</td>
<td>NERC CIP</td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Energy</td>
<td>FIPS, FISMA, NIST 800-53 rev3, HIPPA</td>
</tr>
<tr>
<td>Department of Health and Human Services</td>
<td>Public Health and Healthcare</td>
<td>TBD</td>
</tr>
<tr>
<td>Department of the Interior</td>
<td>National Monuments and Icons</td>
<td>PCI, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Banking and Finance</td>
<td>AWWA &gt;&gt; CFATS</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Drinking Water and Water Treatment Systems</td>
<td>CFATS, NEI-0404, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td></td>
<td>FIPS, FISMA, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Office of Cyber Security and Telecommunications</td>
<td>Information Technology, Telecommunications</td>
<td>FIPS, FISMA, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td>Postal and Shipping</td>
<td>TBD</td>
</tr>
<tr>
<td>Transportation Security Administration, United States Coast Guard</td>
<td>Transportation Systems</td>
<td>FIPS, FISMA, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Immigration and Customs Enforcement, Federal Protective Service</td>
<td>Government Facilities</td>
<td>FIPS, FISMA, NIST 800-53 rev3</td>
</tr>
<tr>
<td>Sector-Specific Agency</td>
<td>Critical Infrastructure/Key Resources Sector</td>
<td>Security Standard</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Department of Agriculture</td>
<td>Agriculture and Food</td>
<td>TBD &gt;&gt; <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Department of Defense</td>
<td>Defense Industrial Base</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Energy</td>
<td>NERC CIP &gt;&gt; <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Department of Health and Human Services</td>
<td>Public Health and Healthcare</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong>, HIPPA</td>
</tr>
<tr>
<td>Department of the Interior</td>
<td>National Monuments and Icons</td>
<td>TBD &gt;&gt; <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Banking and Finance</td>
<td>PCI, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Drinking Water and Water Treatment Systems</td>
<td>AWWA &gt;&gt; CFATS &gt;&gt; <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td></td>
<td>CFATS, NEI-0404, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Office of Infrastructure Protection</td>
<td>Chemical</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td></td>
<td>Commercial Facilities</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td></td>
<td>Dams</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td></td>
<td>Emergency Services</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td></td>
<td>Commercial Nuclear Reactors, Materials, and Waste</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Office of Cyber Security and Telecommunications</td>
<td>Information Technology</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td></td>
<td>Telecommunications</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td>Postal and Shipping</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Transportation Security Administration, United States Coast Guard</td>
<td>Transportation Systems</td>
<td>TBD &gt;&gt; <strong>NIST 800-53 rev3</strong></td>
</tr>
<tr>
<td>Immigration and Customs Enforcement, Federal Protective Service</td>
<td>Government Facilities</td>
<td>FIPS, FISMA, <strong>NIST 800-53 rev3</strong></td>
</tr>
</tbody>
</table>
Standards and Regulations can be overwhelming at times. Seek professional advice if you believe your business may be impacted....
ISA S99 (now referenced in NIST 800-53)

- Four Part Standard
  - ISA S99.00.01 – Models, Definitions, and Terminology
  - ISA S99.00.02 - Establishing a Manufacturing and Control System Security Program
  - ISA S99.00.03 – Operating a Manufacturing and Control Systems Security Program
  - ISA S99.00.04 - Specific Security Requirements for Manufacturing and Control Systems
- (more documents and work products being released soon)

Source: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
## ISA S99 Committee Work Products List

<table>
<thead>
<tr>
<th>ISA Number</th>
<th>IEC Number (proposed)</th>
<th>Work Product Subject</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA-99.01.01</td>
<td>IEC 62443-1-1</td>
<td>Terminology, Concepts And Models</td>
<td>Released</td>
</tr>
<tr>
<td>ISA-TR99.01.02</td>
<td>IEC/TR 62443-1-2</td>
<td>Master Glossary of Terms and Abbreviations</td>
<td>Draft</td>
</tr>
<tr>
<td>ISA-99.01.03</td>
<td>IEC 62443-1-3</td>
<td>Security Compliance Metrics</td>
<td>Draft</td>
</tr>
<tr>
<td>ISA-99.02.01</td>
<td>IEC 62443-2-1</td>
<td>Establishing an IACS Security Program</td>
<td>Released</td>
</tr>
<tr>
<td>ISA-99.02.02</td>
<td>IEC 62443-2-2</td>
<td>Operating an IACS Security Program</td>
<td>Proposed</td>
</tr>
<tr>
<td>ISA-TR99.02.03</td>
<td>IEC/TR 62443-2-3</td>
<td>Patch Management in the IACS Environment</td>
<td>Proposed</td>
</tr>
</tbody>
</table>
### ISA S99 Work Products List continued...

<table>
<thead>
<tr>
<th>ISA Number</th>
<th>IEC Number (proposed)</th>
<th>Work Product Subject</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA-TR99.03.01</td>
<td>IEC/TR 62443-3-1</td>
<td>Security Technologies for Industrial Automation and Control Systems</td>
<td>Released</td>
</tr>
<tr>
<td>ISA-99.03.02</td>
<td>IEC 62443-3-2</td>
<td>Target Security Assurance Levels for Zones and Conduits</td>
<td>Draft</td>
</tr>
<tr>
<td>ISA-99.03.03</td>
<td>IEC 62443-3-3</td>
<td>System Security Requirements and Security Assurance Levels</td>
<td>Draft</td>
</tr>
<tr>
<td>ISA-99.03.04</td>
<td>IEC 62443-3-4</td>
<td>Product Development Requirements</td>
<td>Proposed</td>
</tr>
<tr>
<td>ISA-99.04.01</td>
<td>IEC 62443-4-1</td>
<td>Embedded Devices</td>
<td>Proposed</td>
</tr>
<tr>
<td>ISA-99.04.02</td>
<td>IEC 62443-4-2</td>
<td>Host Devices</td>
<td>Proposed</td>
</tr>
<tr>
<td>ISA-99.04.03</td>
<td>IEC 62443-4-3</td>
<td>Network Devices</td>
<td>Proposed</td>
</tr>
<tr>
<td>ISA-99.04.04</td>
<td>IEC 62443-4-4</td>
<td>Applications, Data and Functions</td>
<td>Proposed</td>
</tr>
<tr>
<td>ISA99 Common</td>
<td>Security Program</td>
<td>Technical - System</td>
<td>Technical - Derived</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>ISA-99.01.01 Terminology, Concepts And Models</td>
<td>ISA-99.02.01 Establishing an IACS Security Program</td>
<td>ISA-TR99.03.01 Security Technologies for Industrial Automation and Control Systems</td>
<td>ISA-99.04.01 Embedded Devices</td>
</tr>
<tr>
<td>ISA-TR99.01.02 Master Glossary of Terms and Abbreviations</td>
<td>ISA-99.02.02 Operating an IACS Security Program</td>
<td>ISA-99.03.02 Target Security Assurance Levels for Zones and Conduits</td>
<td>ISA-99.04.02 Host Devices</td>
</tr>
<tr>
<td>ISA-99.01.03 System Security Compliance Metrics</td>
<td>ISA-TR99.02.03 Patch Management in the IACS Environment</td>
<td>ISA-99.03.03 System Security Requirements and Security Assurance Levels</td>
<td>ISA-99.04.03 Network Devices</td>
</tr>
<tr>
<td>was ISA-99.03.03</td>
<td></td>
<td>was Foundational Requirements was ISA-99.01.03</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA-99.04.04 Applications, Data And Functions</td>
</tr>
</tbody>
</table>

© Copyright Red Tiger Security – Do not print or distribute without consent.
Sample Security Framework - NERC CIP

• Provide a quick overview of the NERC CIP standards

• Allow time for a NERC CIP update at the end
<table>
<thead>
<tr>
<th>Major Functional Areas</th>
<th>NERC CIP Standards</th>
<th>ISO/IEC 17799</th>
<th>API 1164</th>
<th>NIST Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment / Asset Identification</td>
<td>CIP-002</td>
<td>5</td>
<td>B.1, 4.1, 4.1.5</td>
<td>800-30</td>
</tr>
<tr>
<td>Network Management</td>
<td>CIP-005</td>
<td>8.5</td>
<td>3.1,6.1</td>
<td>800-12</td>
</tr>
<tr>
<td>Change Management</td>
<td>CIP-006</td>
<td>10.5.1</td>
<td>B.3.1</td>
<td>800-12</td>
</tr>
<tr>
<td>Access Controls</td>
<td>CIP-003, CIP-004, CIP-005, CIP-006, and CIP-007</td>
<td>9</td>
<td>2, B.3.6.2</td>
<td>800-14</td>
</tr>
<tr>
<td>Governance</td>
<td>CIP-003</td>
<td>4</td>
<td>B.5</td>
<td>800-14</td>
</tr>
<tr>
<td>Incidence Response</td>
<td>CIP-008</td>
<td>6.3</td>
<td>7.2</td>
<td>800-12, 800-14, 800-61</td>
</tr>
<tr>
<td>Information Classification &amp; Handling</td>
<td>CIP-003</td>
<td>5.2.2</td>
<td>4.1.5</td>
<td>800-14</td>
</tr>
<tr>
<td>HR and Personal Risk Assessment</td>
<td>CIP-004</td>
<td>6.1.2</td>
<td>4.1.4,5.1.1</td>
<td>800-14</td>
</tr>
<tr>
<td>Physical Security</td>
<td>CIP-006</td>
<td>7</td>
<td>5</td>
<td>800-12, 800-14</td>
</tr>
<tr>
<td>Recovery Operations</td>
<td>CIP-009</td>
<td>8.4.1</td>
<td>B.3.5.1</td>
<td>800-92</td>
</tr>
<tr>
<td>Systems Management</td>
<td>CIP-007</td>
<td>8</td>
<td>3</td>
<td>800-12, 800-14</td>
</tr>
<tr>
<td>Testing</td>
<td>CIP-007</td>
<td>11.1.5,11.1.5.1-11.1.5.2</td>
<td>B.2.3.5</td>
<td>800-12, 800-14, 800-42</td>
</tr>
<tr>
<td>Training</td>
<td>CIP-004</td>
<td>6.2.1</td>
<td>7.1, B.5.2, B. 5.2.4</td>
<td>800-12, 800-14, 800-50</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>CIP-005, CIP-007</td>
<td>7.1.1, 7.1.5, 7.2.5, 7.2.6</td>
<td>2.1, 5.1.1-2, B.2</td>
<td>800-12, 800-26, 800-42</td>
</tr>
</tbody>
</table>
Framework for Understanding the NERC CIP Standard

All areas of the NERC CIP Standard can be mapped into 14 “Functional Areas”

- Risk Assessment / Asset Identification
- Network Management
- Change Management
- Access Controls
- Governance
- Incidence Response
- Information Classification & Handling
- HR and Personal Risk Assessment
- Physical Security
- Recovery Operations
- Systems Management
- Testing
- Training
- Vulnerability Assessment
NERC CIP Standards Overview

- **CIP-002-1 – Cyber Security – Critical Cyber Asset Identification:** Requires the identification of critical assets and critical cyber assets using a risk-based assessment methodology.

- **CIP-003-1 – Cyber Security – Security Management Controls:** Requires the development and implementation of security management controls to protect critical cyber assets identified pursuant to CIP-002-1.

- **CIP-004-1 – Cyber Security – Personnel & Training:** Requires personnel with access to critical cyber assets to have identity verification, a criminal check, and employee training.

- **CIP-005-1 – Cyber Security – Electronic Security Perimeters:** Requires the identification and protection of an electronic security perimeter and access points that encompass the critical cyber assets.

- **CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets:** Requires a responsible entity to create and maintain a physical security plan to protect cyber assets within an electronic security perimeter.

- **CIP-007-1 – Cyber Security – Systems Security Management:** Requires methods, processes, and procedures for securing critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

- **CIP-008-1 – Cyber Security – Incident Reporting and Response Planning:** Requires identification, classification, and a response plan and reporting of cyber security-related incidents.

- **CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets:** Requires recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.
Risk Assessment / Asset Identification (CIP-002)

Step 1 - Gather information regarding generation resources, substations, control centers, system restoration processes, load shedding, and protection processes to build a list of ASSETS.

Step 2 - Select a Risk Based Assessment process and document that process *(required documentation)*. Use that process to filter this large list down to a list of only those that are CRITICAL ASSETS *(also required documentation)*.

Step 3 - Identify the CYBER ASSETS that support the functions of those critical assets, then filter only those cyber assets that are essential to the operations of the critical assets.

Step 4 - Generate the list of CRITICAL CYBER ASSETS *(required documentation)*. 

**NOTE**: Keep in mind that non-critical cyber assets inside the electronic perimeter must be treated as critical cyber assets.
Network Management (CIP-002/5)

• Step 1 - Identify and document the ELECTRONIC SECURITY PERIMETER (ESP)

• Step 2 - Identify and document all ACCESS POINTS (AP) in and out

• Step 3 - Identify and document all CRITICAL and NON-CRITICAL CYBER ASSETS within the Electronic Perimeter

  • Comments:
    > Don’t forget about DIAL-UP connections
    > Links between perimeters are not considered part of the ESP
    > End points for these links are also considered APs.

• Why is the ESP important?
  • Determines scope for access controls, monitoring, physical protection, and training
  • Drives documentation and log retention requirements

• ESP and all Corresponding Documentation Must be Reviewed Annually
Change Management (CIP-003)

• Most are familiar with Change Management from Corporate requirements, SOX, or other requirements for change management

• Examples of how it is required for NERC CIP Compliance includes:
  • List of Assets, Critical Assets, and Critical Cyber Assets must be documented as changes are made
  • Documented testing required prior to changes made to production systems
  • Patch Management
  • Any changes to the ESP must be put through Change Management
  • Any changes to the Physical Security Perimeter (PSP) must also be documented
  • Any change to the known services/ports allowed on hosts and through access points must also go through Change Management
  • Any change to personnel that have physical access to critical cyber assets
Change Management (CIP-003)

• What Documentation is Required for Change Management (How do you do it?)
  • **Document the Process**
    • Types of change to be made
    • Who will initiate the change
    • Who approves the change
    • Who tests the change
    • Who implements the change
  • **Document the Results**
    • Performance of system after change
    • Any incidents or emergencies caused by the change
Change Management (Tip)

• What if changes are made by outside resources out of my control?

• 1. Vendor / System Integrator
  • Document the Change Management process
  • Create a “cheat sheet” one-page version for vendors with access to the system
  • Require service provider to follow the process
  • Periodically test to ensure that process is being followed

• 2. Enterprise IT Group Responsible for Some Assets
  • They should be following a corporate policy
  • Check to make sure that this corporate policy fulfills NERC requirements
  • Request periodic supporting documentation that Change Management is followed

• 3. Outsourced MSS (Managed Security Services)
  • Outsourced entity can do this for you as a service
Access Controls (5 out of the 8 standards cover this)

- CIP-003, CIP-004, CIP-005, CIP-006, and CIP-007
- Process must be in place to provide access controls to Critical Cyber Assets and any information relating to Critical Cyber Assets
- Management Controls must be reviewed annually
- Documentation must be kept up to date on who has authorized, unescorted, physical access to Critical Cyber Assets

Hint:
- Scope can be reduced by limiting assets within the Physical and Electronic Security Perimeters
- Move non-essential applications and systems out of the ESP and PSP
- Consider installing Critical Cyber Assets in small locked cages or locked cabinets...entire room does not need to be within the PSP (cage creates 6 walls)
Cages and fencing can create the required “6-walls” within the existing Data Center, if Enterprise IT and SCADA/EMS systems are currently in the same room.
Access Controls (Personnel and Remote Access)

• Personnel Implications
  • List of authorized personnel reviewed quarterly
  • Any change to list must be documented within 7 days
  • Change of personnel
  • Change of access rights (initiating or revoking)
  • Personnel Terminated for cause must be documented in 24 hours
  • NOTE: includes Contractors and/or Vendors

• Don’t Forget about Remote Access (included under Electronic Access Controls)
  • Provide challenge/response for any access requested into the ESP
  • Log all attempts (successful and unsuccessful) into the ESP
  • Must be setup as Deny-By-Default...include Appropriate Use Banners where possible
  • Logs to be retained for 90 days / User accounts reviewed annually
Access Controls (Systems Management) – NERC CIP-003

• Requirements for Systems Management should already be in place
  • If not already done so, limit access to and use of Administrator accounts by:
    • Identifying those with access to Administrator and Shared Accounts
    • Limiting access to only those with authorization
    • Require Administrators to log on with their own unique login, not the Administrator account
    • Document the process for changing access levels upon personnel change
    • Always “enable” auditing and logging of any activity performed by Administrator, accounts with Admin privileges, or shared accounts
    • Remove, disable, or rename Administrator accounts wherever possible
    • Change Administrator passwords routinely - especially after personnel or contractor change
Access Controls (Password Management) – NERC CIP-003

- Because of Operational Considerations, Passwords Requirements by NERC CIP will typically be lower than requirements by corporate IT policies
  - Wherever technically feasible, passwords must:
    - Have a minimum of 6 characters
    - Contain a combination of alpha, numeric, and “special” characters
    - Should be changed at LEAST annually, however, should be changed more often based on risk

- Hints:
  - Use of Domain Controllers within the environments supporting Critical Cyber Assets allow for easier system management
  - Changes can be “pushed” out to multiple workstations, once tested
  - All logs can be centrally managed (technology can reduce human labor)
Governance (CIP-003)

• Identifying the “Responsible Entity”
  • Should also extend into identifying the Internal CIP Compliance Team, but documentation of the team is not required, only the “Responsible Entity”
  • Documentation required within 30 days of any change in the “Responsible Entity”
  • Most areas can be delegated, but annual review of the security policy can not be delegated to anyone else

• Cyber Security Policy
  • Policy must address all areas of CIP-002 through CIP-009
  • Can be made up of a group of security policies, but must be able to prove that all areas of NERC CIP compliance is covered across all policies
  • Exceptions to policy can be granted based on emergency conditions
  • Security Policies must be made available publicly
Incidence Response (CIP-008)

- Need to document which types of incidents are classified as a “Cyber Security Incident”
  - Malicious or suspicious events require following the IR plan
  - Normal operational failures not in scope

- Response Plan should include:
  - What events trigger the IR plan
  - Tasks and checklists required to updating
  - Roles and responsibilities required to update the plan
  - Timing and requirements
Trojans infect SCADA system

Problem
A manufacturing company in the U.S. set up a direct link with one of their trading partners. The link bypassed the standard security, and allowed a Trojan onto the plant floor. The Trojan modified existing code on the SCADA system, making cleanup efforts very difficult.

Consequences
Cleanup efforts took two weeks with associated production productivity loss. All code became suspect, requiring reinstalling OS with the potential loss of customizations, configurations, the difficulty of locating original media, replicating original build, and retesting.

Key Control System Recommendations
Technology: Tighter firewall configuration rules, IDS, and IPS/Network Antivirus perimeter protection
Policy: Up to date recovery procedures and media
An email was sent with a Trojan to a PC near the SCADA/DCS Systems, and then the Trojan was remotely controlled from anywhere in the world.

SCADA/DCS systems lacked virus protection software, and this case, the antivirus software was not maintained up to date.

Most SCADA computers we have observed do not have proper security patches installed.
Worm Crashes Offshore Oil/Gas SCADA System Causing $1.2 Million in Loses

Problem
In 2004, two major Oil and Gas Companies both had connections to an offshore production platform to monitor and control 4 large down hole wells. The operator of the platform had very tight strong cyber security, but the other royalty owner was also connected to the platform to get real-time data. The SQL Slammer worm crawled through the royalty owner’s corporate IT network, and onto the platform, and in less than a minute, all operator workstations and SCADA Servers were blue-screened and would not restart after reboot. It took 8 hours to restore the SCADA system and restart production.

Consequences
Immediate loss of monitoring the down-hole wells forced an ESD condition, and loss of production for all 4 major wells. Hard losses in production and pipeline fees totaled over $1.2 million before production was finally restored.

Key Control System Recommendations
Policy: Did not implement a Network Connection Policy for 3rd Parties
Restoration Media and Recovery Process Not Tested

Technology: Missing a Defense-in-Depth Approach, no Antivirus at the perimeter, no IDS, no Antivirus on the Host Computers
Information Classification & Handling (CIP-003)

• **Identify Information that should be protected**...examples include:
  > Operational procedures
  > Lists required for CIP-002
  > Network Topologies
  > Floor plans of computing centers that contain Critical Cyber Assets
  > Equipment layouts of Critical Cyber Assets
  > Disaster Recovery Plans
  > Incident Response Plans

• **Information can be in multiple formats:**
  > Physical Documents
  > Electronic documents
  > Backup media
  > Mobile media (USB keys, CDs, DVDs, disks...)

• **Select a classification system**...examples include:
  > Government - Unclassified, Protected, Confidential, Secret, Top Secret
  > Industry - Public, Internal-only, Confidential, Restricted
  > Use a system that matches the organizations needs
Quick Check - What have we covered so far...

• All areas of the NERC CIP Standard can be mapped into 14 “Functional Areas”
  > Risk Assessment / Asset Identification
  > Network Management
  > Change Management
  > Access Controls
  > Governance
  > Incidence Response
  > Information Classification & Handling
  > HR and Personal Risk Assessment
  > Physical Security
  > Recovery Operations
  > Systems Management
  > Testing
  > Training
  > Vulnerability Assessment
HR and Personal Risk Assessment (CIP-004)

- Required Checks:
  - Identity verification
    - Form I-9 for the US
    - Canada developing similar verification
  - Seven year criminal check
    - Includes local, county, state, federal, and sex offenders registration
  - Can conduct more detailed reviews
    - (Employment history, education, credit checks...)

- Criminal Check Considerations:
  - Responsible Entity should predefine what actions are considered “adverse”
  - Describe and list company liabilities for actions based on adverse information
  - Existing employee process vs. New hire process
• Rinse and Repeat
  • Update each personnel risk assessment at least every seven years or for cause
  • Company should provide managers with parameters to a “for cause” check
  • Supporting documentation must also be keep for “contractor and service vendor personnel”

• HINTS:
  • Make sure to include representation from HR when setting policy that impact personnel privacy
  • There may be implications when represented workers are involved
Physical Security (CIP-006)

- Physical Security Plan
- Physical Access Control
- Monitoring Physical Access
- Logging Physical Access
- Access Log Retention
- Maintenance and Testing
Physical Security (CIP-006)

- Starts with having and documenting a Physical Security Plan
- Similarities to Cyber
- **Know your Perimeter** (Hint: Remember small cages can still create the required “6-walls”)
- **Know your Access Points** (must manage access into PSP with 24x7 coverage)
- **Know your Procedures** (access rights, escorted / unescorted access, termination)
- **Know your Controls** (see list below, some include multi-factor authentication)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Key</td>
<td>Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.</td>
</tr>
<tr>
<td>Special Locks</td>
<td>Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.</td>
</tr>
<tr>
<td>Security Personnel</td>
<td>Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.</td>
</tr>
<tr>
<td>Other Authentication Devices</td>
<td>Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.</td>
</tr>
</tbody>
</table>
Physical Security - Monitoring / Logging (CIP-006)

Just like Cyber, Physical Access Monitoring is also Important

<table>
<thead>
<tr>
<th>Monitoring Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computerized Logging</td>
<td>Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method.</td>
</tr>
<tr>
<td>Video Recording</td>
<td>Video Recording: Electronic capture of video images of sufficient quality to determine identity.</td>
</tr>
<tr>
<td>Manual Logging</td>
<td>Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.</td>
</tr>
<tr>
<td>Access Log Retention - 90 Days</td>
<td>Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.</td>
</tr>
<tr>
<td>Maintenance and Testing</td>
<td>Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:</td>
</tr>
</tbody>
</table>
Recovery Operations (CIP-009)

• Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.
  • First Step? - Establish your Recovery Plan
  • Procedure to specify actions in response to event/conditions that would activate the plan
  • Definition of responder roles and responsibilities
  • Annual recovery plan exercise procedure
  • Recovery Plan change control procedure
  • Backup and Restore procedure
  • Backup media test procedure
  • Use a reliable tape rotation schedule, and routinely check for restore capability
Systems Management (CIP-007)

• Ports and Services
  • Document known ports and services and only enable those required for normal and emergency operations
  • Disable unused ports and services
  • NOTE: It helps to capture traffic for 10 to 15 minutes first to see what the typical ports and setting are in use

• Security Patch Management
  • Track with security patches for Critical Cyber Assets have been released
  • Evaluate if there are compelling reasons not to patch and document them
  • Test the patches on development systems first
  • Document the implementation of security patches
Systems Management (CIP-007)

- **Malicious Software Prevention**
  - The responsible party shall use anti-virus software and other malware prevention tools to detect, prevent, deter, or mitigate the exposure to propagation of malware
  - **HINT:** It is easier to deploy and maintain antivirus-on-the-wire at the perimeter than on the systems within the perimeter

- **Security Status Monitoring**
  - Security monitoring controls shall issue automated or manual alerts when they detect something out of the norm
  - Processes for enabling ports on hosts, routers, and firewalls
  - Alerts generated by the monitoring solution should be logged
  - Logs must be maintained for a minimum of 90 days
  - **HINT:** Security Monitoring, Alert Correlation, Central Log Retention, and reporting can all be automated using technology - goal is to reduce human labor
Testing (CIP-007)

• Do you have procedures for TESTING your systems?

• A significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
  • Step 1 - Create the procedures
  • Step 2 - Test the procedures to ensure they are being followed
  • Step 3 - Document the rests from testing the procedures

• Document the test results
  > Perform “port scans” to identify open/available services
  > Check the file integrity to identify change in certain files
  > Review technical documentation for solutions to determine security features

• Testing should be integrated into the change management process

• Just like SOX, results from the testing of security controls must be documented
Training - General Security Awareness (CIP-004)

• Security Awareness Training is less rigorous, less detailed, and the content is left up to the utility
  > Examples include:
    > Password usage, management, shoulder surfing, tailgating, etc..
    > Unknown emails, attachments, spam, phishing
    > Social engineering techniques
    > Incident response
    > Access controls

• Training can be delivered through:
  > Direct Methods - Emails, Memos, Computer-based training
  > Indirect Methods - Posters, Intranet, Brochures
  > Management support and reinforcement - presentations and staff meetings

• Awareness training should be reinforced on a quarterly basis

• Most utilities should already be doing this
Training - Specific Training Courses (CIP-004)

- Unlike general security awareness training, this training content is specified and must be more detailed, and based on access to critical cyber assets.

- Required content should include:
  - Proper use of Critical Cyber Assets
  - Concept of the Physical and Electronic Security Perimeter(s)
  - Proper handling of Critical Cyber Asset information
  - Action plans and procedures to recover Critical Cyber Assets and access following a Cyber Security Incident

- **NOTE:** Having the training materials is the only proof required for the awareness training program.

- **NOTE:** The job-specific training courses have greater requirements to show proof:
  - Attendance records
  - Date when training was provided
  - Proof training was conducted at least annually
  - Documented training materials
Vulnerability Assessment (CIP-005, CIP-007)

• **Assessment process should include:**
  • Access into the Electronic Security Perimeter through Access Points (Perimeter)
  • Vulnerability Assessment of Cyber Assets within the perimeter (internal systems)

• **VA process should include:**
  • **Documentation** of the assessment methodology for:
    • Access points to the Electronic Security Perimeter (Perimeter)
    • The cyber assets inside the perimeter
  • At a minimum, this process / methodology should include:
    • Only those ports and services required for system operations are enabled
    • Required open ports may need additional security if services are vulnerable
    • Discovery of all access points
    • Review of the access controls, passwords, and network management
    • Methodical process for covering all cyber assets from the perimeter down to the lowest component in the system
Security Mapped to 6 Functional Areas

1. Physical Access
   (Limit Direct Access to Control Rooms and Equipment)

2. Network Architecture
   (Firewalls, Routers, Switches, Network Segmentation, etc.)

3. SCADA DMZ
   (Data Historians, Web Servers, Patching Servers, AV Servers, etc.)

4. Assessing Mission Critical Servers/Workstations for Host and Application Vulnerabilities
   (Operating System settings for SCADA Server(s) and Workstation(s). This includes Domain/Workgroup settings, Active Directory, Group Policy Settings, and critical applications like HMI, CEMS, SCADA, and others.)

5. Control System COMM
   (wired and wireless communications from control room out to local controllers)

6. Local Controllers
   (PLCs, RTUs, IEDs, and any other local control devices)
1. Physical Security
   (Fencing, Surveillance, Guards, Gates, Locks)

2. Network Infrastructure
   (Switches, Routers, Firewalls, 3rd Party Connections, and Modems)

3. Manufacturing IT DMZ
   (Data Historians, Data Logging, Web Servers)

   (Operating System Security, Application Security)

5. Communications to Field Devices
   (Profibus, Modbus, OPC, and other protocols...)

6. Field Devices
   (PLCs, RTUs, IEDs, Plant Equip.)

**Procedural Controls**

Across all Six Layers spans the need for procedural controls that include:
- Asset Inventory, System Documentation, Management of Change, and Test / Development Systems
- Risk Management, Patch Management, Lifecycle Planning, and Routine Assessments
- Crisis Management, Emergency Planning, Safety, and Safe Shutdown Procedures, Backup and Recovery
<table>
<thead>
<tr>
<th>Standards, Policies, or Procedures that Map to the Controls</th>
<th>NERC CIP REQUIRED</th>
<th>CFATS (DHS) REQUIRED</th>
<th>CHEMICALS STANDARD</th>
<th>ISA 999 INTERNATIONAL BEST PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. PHYSICAL SECURITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physically Secure Access to Control Devices - Secure physical access to control system components that monitor or control chemical processing, chemical storage, or transportation.</td>
<td>CIP-005</td>
<td>RBPS 2 - Secure Site Access, RBPS 3 - Screen and Control Access, and RBPS 4 - Detect, Delay, and Countermeasures.</td>
<td></td>
<td>ISA-TR99.00.002, 6.6.1.1. Safety and Environmental Security.</td>
</tr>
<tr>
<td>Physically Secure Access to Control Networks - Control Networks and Field Networks should be physically secured. All critical cyber devices that are used for monitoring or control must be physically secured with 6-walls of protection (i.e., fencing, cages, walls, etc...)</td>
<td>CIP-006</td>
<td></td>
<td></td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
</tr>
<tr>
<td>Role-based Physical Access Controls - Prevent physical access to control system equipment - The facility should have role-based physical access controls to restrict access to critical cyber systems and information storage media.</td>
<td>CIP-008</td>
<td></td>
<td></td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
</tr>
<tr>
<td>Visitor Controls - The facility has documented and implemented visitor identification, escort, and access control procedures that include verification of visitor background suitability or constant visitor escort by appropriately vetted personnel in restricted areas.</td>
<td>CIP-001</td>
<td>Metric 7.3 - Visitor Controls</td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
<td></td>
</tr>
<tr>
<td>Inspection and Testing of Physical Controls - The facility has written procedures, including responsibilities, tasks, and frequencies, to regularly inspect, test, calibrate, repair and maintain security systems (e.g., gates, cameras, lights, alarms, keypad entry systems) and related equipment such as communications and emergency notification equipment.</td>
<td>CIP-005</td>
<td>Metric 10.1 - Inspection, Testing, and Preventative Maintenance (ITPM) Procedures</td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
<td></td>
</tr>
<tr>
<td>Temporary Physical Security During an Outage - Appropriate temporary security measures are implemented in response to non-routine outages, equipment failures and malfunctions, and such incidents are documented and promptly reported to the Site Security Officer.</td>
<td>CIP-008</td>
<td>Metric 10.2 - Outages</td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
<td></td>
</tr>
<tr>
<td>Written Plan to Repair Physical Security Deficiencies - The facility has a written plan to record and repair deficiencies in security-related equipment.</td>
<td>CIP-001</td>
<td>Metric 10.3 - Repairs</td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
<td></td>
</tr>
<tr>
<td>Identification of Security Maintenance Personnel - The facility has procedures to verify the identity and each occurrence of contractor personnel who perform inspection, testing, and maintenance of security equipment</td>
<td>CIP-009</td>
<td></td>
<td>ISA-TR99.00.002, 6.6.1.1. Physical and Environmental Security.</td>
<td></td>
</tr>
<tr>
<td>2. Networking Architecture (Firewalls, Routers, Switches, Hubs)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewalls - A manufacturing process control network must be segregated from the so-called DMZ by an inner firewall. The DMZ must also be segregated from the corporate IT network through an outer firewall.</td>
<td>CIP-005</td>
<td>Metric 8.3.3 - Access Control Lists</td>
<td>ISA-TR99.00.002, 6.6.2.3 Network Access Control.</td>
<td></td>
</tr>
<tr>
<td>Typical Network Traffic - All authorized non-local communications with the process control network shall be through one or both of the DMZ firewalls, depending on the impact of a breach from external access.</td>
<td>CIP-005</td>
<td>Metric 8.2.2 - External Connections</td>
<td>ISA-TR99.00.002, 6.6.2.3 Network Access Control.</td>
<td></td>
</tr>
</tbody>
</table>

web: redtigersecurity.com
### Vulnerability Assessment Reporting

(CIP-005, CIP-007)

**Vulnerability**: ICMP is not filtered at the Access Points

<table>
<thead>
<tr>
<th>Find #</th>
<th>Vulnerability</th>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2. ICMP is not filtered at the Access Points</td>
<td>![Severity Level]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>The firewall device configurations showed that ICMP protocol is being allowed from the outside of the firewall.</td>
<td>While ICMP protocol is typically enabled to allow system administrators to “ping” devices for troubleshooting purposes, it also allows attackers to build covert tunnels that bypass firewall rules. Heavy amounts of ICMP packets has also been known to crash SCADA applications and embedded devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Systems Affected</th>
<th>Recommendations</th>
<th>Level of Effort</th>
<th>Response / Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>All firewall devices reviewed</td>
<td>Disable ICMP protocol from the public or outside interface of the firewalls. If a network monitoring application requires ICMP to work through the firewall, then limit the protocol to work only from a known documented source IP address.</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>
Session Summary Points

- Provided an overview of the US NIPP (National Infrastructure Protection Plan)
- Mapped the US Government Agency Oversight to each Critical Infrastructure Sector
- Provided a current status of various SCADA Security references for adaptation by International markets
- NERC CIP, ISA SP99, CFATS, API 1164, NIST 800-82, NIST 800-53 rev3, AGA 12, CSSP DHS Best Practice Guides, etc...
- Used NERC CIP as a sample security framework to understand the compliance requirements for the Energy sector
- Looked at a few actual security Incidents involving SCADA and Industrial Control Systems
- Finished up with a review of the SCADA VA methodology taught earlier in the course, and how it satisfies the VA requirements in NERC CIP and CFATS