NERC CIP Compliance Program Design, Implementation & Controls, and Metrics & Measurements

Tuesday, February 25, 2014, 1:15PM - 2:45PM

Jerome Farquharson  
Email: jfarquharson@burnsmcd.com  
Phone: 314.737.2744

Compliance & Infrastructure Protection, Burns & McDonnell Engineering Company Inc.

Agenda

• Presenters
• Purpose
• NERC CIP Program Design
• NERC CIP Program Implementation & Controls
• NERC CIP Program Metrics & Measurements
• Final Q&A
Presenters

Jerome Farquharson – Leader of Burns & McDonnell’s Saint Louis Security Practice, CISSP, CRISC
Leader of Burns & McDonnell’s Saint Louis security practice. He leads with a multi-disciplined background of cyber and physical security, information systems and business advisory consulting in all areas of NERC CIP Compliance. Mr. Farquharson is an experienced Security Network Engineer with 21 years IT experience that includes experience in Network Design Implementation, Support and Troubleshooting of CISCO Routers, Switches, Firewalls, VPN Devices, Intrusion Detection Systems and network management systems.

Ingrid Rayo – Sr. Compliance Analyst
Ms. Rayo is a NERC CIP Compliance Program Consultant assisting clients in developing a solid sustainable NERC CIP Program which included a Sabotage Reporting Procedure, Cyber Security Policy, Internal Compliance Program, and other required policies, procedures, and processes associated with CIP-003 through CIP-009 for versions 2 and 3. She has developed a CIP organizational structure conducive to the entity’s size and registration; conducted audit and spot check preparation activities, such as SME workshops, Mock Audits, pre-audit assessments and evidence staging; and drafted Technical Feasibility Exceptions for cyber assets that could not comply with CIP-005 and CIP-007 requirements.
Purpose

Understanding the operational environment, depth of CIP knowledge of operations staff and availability of compliance tools is critical for designing an implementable NERC CIP Compliance Program.

As such, an engineering operations centric design that focuses on key “pillars” of compliance: **Processes, People, Systems and Documents** can lead to a successful implementation of a compliance program in Substations and Power Plants. We will discuss actual implementation of meeting CIP compliance.
NERC CIP Program Design

- Pillars of Compliance
- Compliant Process
- Compliant People
- Compliant System
- Compliant Documentation

GOVERNANCE AND ENFORCEMENT
NERC CIP Compliance Program

Pillars of Compliance
Ensure NERC CIP Requirements are integrated into all business activities

Collect evidence at each logical break or transition in a business process

Example: Prior to commissioning cyber asset

- Disable Factory Accounts
- Disable Unneeded Ports and Services
- Configure Log Collection
- Document Security Test Procedures (for new devices)
Compliant People

Define and Periodically Reinforce

- CIP Board
- Directors and Managers
- Subject Matter Experts
- Implementers

Compliance

- Governance
- “What” and “Who”
- “When” and “Who”
- “How”

Develop compliance program w/ SMEs

Training

- Keep it simple
- Make it relevant
- Show benefits and consequences

Hire CIP Staff with at least two subject areas:

- Utilities Operations
- Cyber Security
- Audit and Compliance
Compliant Systems

Ensure systems support compliance

Asset Management System
- CIP-002, CIP-005, CIP-007, and CIP-009 compatible

Change and Configuration Management System
- CIP-010

Learning Management System
- CIP-004 compatible

Document Management Systems
- CIP Hierarchy compatible

Compliant Documents

Plan
  - Policy
  - Process
  - Procedure
  - Implementation

General Statement of Purpose + Strategy
Specific instance of the relationship between a distinct area of activity that affects information and the overall strategy. A policy is a high level description of recommended security controls for regulating use.

The set of precise actions, tasks, which need to be taken by users in connection with a particular policy.

Technical details of enacting a Policy/Process combination.

Evidence to prove completion.
Compliant Documents

Documentation Responsibilities:

- CIP Steering Committee
- Directors and Managers
- Subject Matter Experts
- Implementers

- CIP Procedures
- CIP Processes
- CIP Evidence Templates
- CIP Policies
- CIP Plan
- Steering Committee Charter

NERC CIP Program Implementation & Controls

- Implementation
- Collaboration
- Cohesiveness
- Transparency
- Controls – Business Operations
- Controls – Evaluate
- Controls – Internal Audits
- Risk Management
Implementation

• Create and improve compliance knowledge and understanding
• Integrate compliance “as part of the job”
• Promote a culture committed to “Excellence”. Do not focus on the minimum.
• Establish an education and outreach program
• Lead by example

Implementation

• Develop a culture of accepting change
• Use effective communication opportunities
  • Employee (Staff) Meetings
  • Lessons Learned
  • On the Job (role) Training (OJT)
  • Lunch and Learn
• Take the show to the road
  • Plant Engineers / Operators / Technicians
  • Substation Engineers / Operators / Technicians
  • Control Room Supervisors and Operators
  • Corporate and Office support personnel
Implementation

Cyber Assets

Events: Processes People Systems Documents

NERC CIP Program

Compliance

NERC Compliance
- Compliance
- Audit Ready

- Critical Infrastructure Protection
- Functional Business Operations
- Cohesiveness, Collaboration and Transparency

Collaboration

- Create CIP Board with representation from each affected Business Unit
- Identify SMEs for each Business Unit/Dept.
  - Control Systems
  - Plant/Substation Assets
  - Corporate Security
  - Information Technology
- Relief compliance burden from SMEs by providing compliance support staff for:
  - Interpretation, guidance, and administration
  - Evidence collection and RSAW preparation
  - Education and training
Cohesiveness

- Educate and empower identified SMEs
- Establish common methodologies with SMEs and each department’s:
  - Processes
  - Systems
  - People
  - Documentation Methodology
- Define and establish CIP specific job roles and responsibilities
- Create compliance and cyber security glossary (Ex: Ports & Services, Account Management, Access Request)

Transparency

- Educate on compliance activities
  - Equipment
  - Personnel
- Build upon integrity and openness - “nothing to hide”
- Clearly determine what evidence is necessary for compliance
- Speak and communicate using conforming Utility Operations Language
- Ownership and accountability
Business Operations

• Bring technical experts along, interview SMEs
• Assess Business Operations vs. CIP Policies, Processes and Procedures
• Evidence collection (Work Forms, Work Tasks, Asset Inventory Details, etc.)
• Establish compliance enhancement or corrective action plans for integration; then execute

Evaluate

Use real scenarios to evaluate compliance

• Assets
  • Change and Configuration Management
  • Commissioning and Decommissioning
  • Recovery and Incident Response
  • Access Management (Physical and Electronic)
  • Information Management
• Personnel
  • PRAs
  • Access Requests
  • Role Specific Training and Security Awareness
  • Access Removal
Internal Audit

- Involve internal auditors (Compliance Expertise)
- Identify and foster levels of authority thru CIP Board
- Perform random and unannounced spot checks

Internal Audit

- Highlight Business Unit’s “Best Practices”
- Reward by recognition
- Establish and publish internal compliance dashboard
- Seek and accept relevant feedback
NERC CIP Program Metrics & Measurements

- Understand the Purpose of Metrics
- What are Metrics and Measures
- Building Metrics
- Developing Metrics
- Metric Attributes
- Metric Examples (Process, People, System, Documents)

Tried and True Adage

Adversaries attack the weakest link.

Where is your weakest link?

People Processes Systems Documents

Metrics will help you identify your weaknesses!
Purpose of Metrics

• Measure the effectiveness of CIP Program
• Monitor progress toward goals
• Expose non-conformance to processes
• Catalyst for improvement to and enhancement of the CIP Program
• Valuable insight which can impart a level of comfort with regard to compliance

Why

A metric is a standard of measurement.

Various types of metrics:
• Strategic
• Performance
• Operational
• Compliance
• Cyber security technical

Blended use of these different metrics depicts the effectiveness of a compliance program.
Developing Metrics

1. Define metrics based on goals and objectives

2. Implement metrics in a manner that encourages the utilization of appropriate tools

3. Monitor established metrics frequently

4. Assess goals and objectives based on monitoring activity

5. Constantly communicate and educate all stakeholders
Metric Attributes

Compliance Pillar
Domain
Purpose
Protocol

Risk
Unit
Strength & Weakness
Data

Collection Process
Tools
Frequency
Goal

Process Metric Example

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Access</td>
</tr>
<tr>
<td>Purpose</td>
<td>Determine &amp; minimize the number of Access Points to an ESP</td>
</tr>
<tr>
<td>Protocol</td>
<td>CIP-005 Electronic Access Point policy requires business units to minimize the number of communication channels into an Electronic Security Perimeter.</td>
</tr>
<tr>
<td>Risk</td>
<td>Minimizing the number of access points reduces accessibility risks.</td>
</tr>
<tr>
<td>Unit</td>
<td>Device Count (Total number of Access Points)</td>
</tr>
</tbody>
</table>
| Strength & Weak | Strength: Identify potential attack paths  
|               | Weakness: Necessity of numerous ESP access points isn't consistent |
| Data         | Network scan results, network configuration, and ESP diagram |
| Collection Process | Utilize approved network scanning tools, only if operations will NOT be impacted, to identify electronic access points.  
|               | Review current version of the ESP diagram(s) |
| Tool(s)      | Approved Network Scanner (Nmap) |
| Frequency    | Monthly |
| Goal         | Less than 5 Electronic Access Points to a single ESP |
# People Metric Example

## Tailgating Count

<table>
<thead>
<tr>
<th>Pillar</th>
<th>People</th>
<th>Domain</th>
<th>Physical Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Determine and minimize the number of tailgating incidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>CIP-006 Control Center Physical Security policy requires each Control Center Employee, including Contractors, to present appropriate credentials at each physical entry portal to the Control Center floor before entering. Employees are prohibited from allowing other individuals to enter the Control Center without appropriate authorization.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>Eliminating tailgating activities reduces physical accessibility risks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Unit</strong></td>
<td>Incident Count (Total number of tailgating incidents from Corporate Security)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Strength &amp; Weak</strong></td>
<td>Measurable by review of video feed and self-reports. All incidents may not be properly captured lending to the metric weakness.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>Video Recordings and physical security door logs depicting open portals greater than 15 seconds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Collection Process</strong></td>
<td>Request video feed &amp; portal logs for 30 day span from previous review. Using the portal logs, extract the entry attempts that exceed 15 seconds. Review the coinciding video feed for the identified access attempts longer than 15 seconds to ensure that only ONE authorized BMcD Employee/Contractor entered the Control Center.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tool(s)</strong></td>
<td>Video Player</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>Monthly</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Goal</strong></td>
<td>Zero Tailgating Incidents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# System Metric Example

## Unapproved Completed Changes

| Pillar  | System | | |
|---------|--------|-------------------|
| **Domain** | Change Control | | |
| **Purpose** | Determine the number of changes made to cyber assets without the appropriate approvals in the Change and Configuration Management System. | | |
| **Protocol** | CIP-003 Change and Configuration Management System Policy; Cyber Asset Change Management Process; Change and Configuration Management System Workflow | | |
| **Risk** | Reducing the number of unauthorized changes reduces reliability risks. | | |
| **Unit** | Incident Count (Total number of unauthorized changes completed) | | |
| **Data** | Change Request records from the Change Management System | | |
| **Collection Process** | Audit the completed and closed change request tickets and ensure the proper approvals were obtained before the change was implemented. | | |
| **Tool(s)** | Change Management System | | |
| **Frequency** | Monthly | | |
| **Goal** | Zero unauthorized changes | | |
Document Metric Example

<table>
<thead>
<tr>
<th>Pillar</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Administrative Control</td>
</tr>
<tr>
<td>Purpose</td>
<td>To determine if the current process has been documented and approved.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Corporate Document Maintenance Program</td>
</tr>
<tr>
<td>Unit</td>
<td>Occurrence Count (Number of documents posted but not approved)</td>
</tr>
<tr>
<td>Data</td>
<td>Document Repository Items</td>
</tr>
<tr>
<td>Collection Process</td>
<td>Review the compliance documents in the document repository and ensure they have been approved.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Goal</td>
<td>Zero Occurrences</td>
</tr>
</tbody>
</table>

Discussions

Send Questions and Comments to Cybersecurity@burnsmcd.com

Thank You!