Changes since video was filmed...

• Page 3 – Audit period for subsequent audits is from the last day of the previous audit through the current audit

• Page 4 – The current audit scope is posted here: Current Compliance Program

• Page 6 – Registered Entities that do not own Critical Assets are no longer required to hash files

December 2013
CIP Audit: What to Expect

Leesa Oakes
Compliance Specialist II - CIP
loakes.re@spp.org · 501.614.3274
Audit Overview

• **Audited Standards/Requirements** based on CIP registered functions, Critical Cyber Assets

• **Audit Period:** October 1, 2010 until date of audit

• **Audit Cycle:** 3-year (BA, TOP, RC) and 6-year (IA, GO, GOP, LSE, TO, TSP)

• **Pre-Audit:** Notification, Request for information, Review of evidence, Supplemental requests (random sampling)

• **Audit:** Opening presentation, Interviews, Review of Evidence, Site Inspections, End-of-day briefings, Exit Presentation

• **Post Audit:** Draft audit report, Entity comments, Feedback forms, Final audit report (non-public)
CIP Audit Scope

• Tier 1 mandatory; we may add from Tier 2 and Tier 3
• We send in-scope requirement list
• Terminated, Approved TFEs
• Open Mitigation Plans
• Scope may be adjusted based on
  – Prior spot check results, self-reports, self-certifications
  – Entity compliance history/reliability statistics
  – Tier 2 and Tier 3 requirements foundational to Tier 1
• Scope may be expanded during the audit
Evidence Request & Inventory Workbook

- Official record of submitted evidence
- Send to us with each evidence submittal
- One workbook for each standard
- One sheet per main level requirement with evidence list
Evidence Request & Inventory Workbook

CIP Compliance Audit Evidence Request and Inventory
Confidential, Non-Public Information

Entity - NCR00000 - Jan 3-28, 2012
CIP-002-3: Critical Cyber Asset Identification
Requirement R3: Critical Cyber Asset Identification

Initial Evidence Requested:
(P) = Primary evidence; (S) = Supporting Evidence

R3 (Tier 1):
1) (P) Approved list of Critical Cyber Assets
2) (P) Evidence that the Critical Cyber Asset list is reviewed at least annually
3) (P) Evidence that the Critical Cyber Asset list is updated as necessary
4) (S) Approved list of Critical Assets
5) (S) List of Cyber Assets considered for inclusion on the Critical Cyber Asset list (include containing Critical Asset or facility, brief functional description)

Evidence to be Randomly Sampled:
- None -

Evidence Provided:

<table>
<thead>
<tr>
<th>Document File Name</th>
<th>Description</th>
<th>Page Ref.</th>
<th>SHA-2(256) Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSAW CIP-002-3 (September 2011).doc</td>
<td>Compliance Questionnaire and Reliability Standard Audit Worksheet</td>
<td>All</td>
<td>500d0d67afa9affce4681ef65963bcff96b6e013eb46ead8fd16d05640c19d94</td>
</tr>
<tr>
<td>CCA Review_10152011.doc</td>
<td>Annual review of Critical Cyber Asset list</td>
<td>Page 1</td>
<td>3eefa1f678d05c31c0ed278c431bc55d971c4a022875704702041595116df726</td>
</tr>
</tbody>
</table>
You complete RSAW for each Standard

- RSAWs included in audit packet are pre-populated with audit team and entity information
- Provide detailed narrative of how you meet compliance for each requirement
- For evidence you may reference the *Evidence Request & Inventory Workbook*

*Best practice:*

- Complete all applicable RSAWS for Tier 1, 2, and 3
- Hold those labeled *not required in initial audit notice* in case SPP RE requests them as part of audit scope expansion
- Be prepared to provide evidence for Tier 2 and 3 in case audit scope is expanded
RSAW example

R2. Ports and Services — The Responsible Entity shall establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

Describe, in narrative form, how you meet compliance with this requirement:
(Registered Entity Response Required)

Acme Inc. has a documented process for ensuring that only those ports and services required for normal or emergency operations are enabled (see CIP007-R2_Ports and Services Procedure_2012.pdf). Acme Inc. implements this process by running a port scan after any changes to identify any unapproved ports.

Acme Inc. maintains lists of approved ports and services that have been identified through vendor documentation and discussion, research, and results of port scans (see CIP-007-R2_Baseline).

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>See CIP-007-3 Evidence Request Workbook, sheet R2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You provide preliminary evidence lists:

A. Critical Assets

B. Cyber Assets subject to CIP standards (CCAs) identified as either existing or newly implemented during audit period
   
   B1. Critical Cyber Asset,
   
   B2. Other Cyber Asset within the Electronic Security Perimeter,
   
   B3. Cyber Asset performing Electronic Access Control, Monitoring, and/or Alerting, or
   
   B4. Cyber Asset performing Physical Access Control, Monitoring, and/or Alerting,

C. Personnel with authorized electronic or authorized, unescorted physical access to CCAs

D. Uniquely identified patches/security updates applicable to one or more Cyber Assets subject to CIP standards
You provide preliminary evidence lists:

E. Significant changes made to any of the Cyber Assets subject to testing requirements of CIP-007-3, Requirement R1

F. Uniquely identified Physical Access Control Points

G. Local/domain user accounts defined or enabled for use on one or more Cyber Assets subject to the CIP standards
   G1. Administrator privileged account
   G2. Generic system account
   G3. Shared user account, and/or
   G4. Individually assigned user account.
Preliminary evidence lists

• Critical Asset list
  – List physical address related to each asset

• Significant changes
  – List associated implementation dates

• Cyber assets
  – List associated ESP, if it’s within one, and associated PSP

• Physical access points
  – List physical location, associated Critical asset and monitoring method
We complete Random Sample Matrix

- We use statistical tool (RATSTATS) to determine sample size and select random samples from your preliminary evidence lists
  - 95% confidence level, 5% error, 0.5% probability of occurrence
- We populate Random Sample Matrix and send to you
- You will pull evidence related to Random Sample Matrix lists and send to us
- Only entities with CCAs will have random samples
RANDOM SAMPLE MATRIX DEMO
Compliance Audit Process

1. Opening presentation
2. Interviews with Subject Matter Experts (SMEs)
3. Outreach
4. Review of evidence
5. Physical site inspection (onsite audit only)
6. End of day briefings (onsite audit only)
7. Exit presentation
8. Entity maintains evidence copy of record (onsite audit only)
Post-Audit Process

- RE Management and Enforcement review
- Draft audit report
  - 4 weeks after audit
- Entity comments
  - 15 days to review/comment
- Feedback forms
- Final (non-public) audit report to NERC and entity
  - 75 days after end of onsite audit (60 days for offsite audit)
Audit report Recommendations and Areas of Concern

• Recommendations
  – Requirement specific:
    ▪ Implementation of patches
    ▪ Additional testing of Physical Access Control System

• Areas of Concern
  – Over-arching issues, not requirement specific:
    ▪ Also print the name of a document signatory
    ▪ Lack of specificity in documentation overall
Preparing for a Successful On-Site Audit

1. Organize your evidence by standard and requirement
   – If artifact applies to multiple requirements, place copy in each folder
2. Know your evidence – be prepared to explain it
3. Don’t hold back by trying to provide only the minimal amount you think the auditors are looking for
4. Make sure the interview room is ready
5. Do a mock audit
References

- **SPP.org > Regional Entity > Compliance & Enforcement**
  current year Compliance folder on left for annual SPP RE:
  - Audit Scope Plan
  - Implementation Plan
  - Evidence Request and Inventory workbooks
  - Random Sample Matrix
Leesa Oakes
Compliance Specialist II - CIP
loakes.re@spp.org · 501.614.3274