Helping our members work together to keep the lights on... today and in the future
Overview of CIP
Audit Timelines and Evidence Requests

March 18, 2011

Shon Austin
Senior Compliance Specialist - CIP
saustin@spp.org · 501.614.3273
Agenda

• Overview
• Initial Notice
• Audit Package
• Evidence Request and Inventory Workbooks
• Audit Logistic
• Post Audit
Overview

• **Audited Standards/Requirements** are based on CIP registered functions

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

• **Audit Cycle:** 3-year and 6-year

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

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

• **Post Audit:** Draft audit report, Entity comments, Feedback forms, Final audit report (non-public and public versions)
Initial Notice

• Notification Letter
  – Audit Dates
  – Audit Scope
  – Overview of Audit Process
  – General Description of Audit Package
    ▪ Q/RSAWs, Compliance Survey, Request for Initial Evidence, etc.
Audit Package

• List of Audit Team Members
  – Professional Bio’s for the Audit Team Members
  – Codes of Conduct
  – Work History/Conflict of Interest Forms
• Verification of Recent Employment
• Pre-Audit Survey & General Information Questionnaire
• Audit Information Certification Letter
Audit Package

• General Information
  – NERC Compliance Process Bulletin #2009-004
  – NERC Audit Information Certification Letter
  – NERC Questionnaire and Reliability Standards Worksheets (Q/RAWs)
  – References to Other Resources
    ▪ NERC Annual CMEP Plan
    ▪ NERC Actively Monitored Standards List
Audit Package

• Initial Request for Evidence
  – Instructions
    ▪ Meeting Submission Deadlines
    ▪ Organizing Evidence Files
    ▪ Completing and Maintaining Evidence Request and Inventory Workbook
    ▪ Marking and Handling of Confidential Data
Submission Deadlines

• 60 Days prior to the scheduled audit
  – Verification of Audit Team Members COI Forms

• 45 Days prior to the scheduled audit
  – Executed Compliance Audit Information Certification Letter
  – Completed Pre-Audit Survey/Questionnaire
  – Completed Q/RAWs
  – Initially Requested Evidence
  – Completed Evidence Inventory Workbook

• 15 Days prior to the scheduled audit
  – Objection to Audit Team Member
Organizing Evidence Files

- Separate Folder for Each Standard
- Separate Subfolder for Each Requirement
Evidence Request and Inventory Workbook

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

Entity - NCR00000 - Jan 3-28, 2011
CIP-002-3: Critical Cyber Asset Identification
Requirement R3: Critical Cyber Asset Identification

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

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 (January 2011).doc</td>
<td>Compliance Questionnaire and Reliability Standard Audit Worksheet</td>
<td>All</td>
<td>ff5092b052d08a3eaa6e5c048501342544694709c310d2d9946b3e089c0ef95e</td>
</tr>
<tr>
<td>CCA Review_03012010.doc</td>
<td>Annual review of Critical Cyber Asset List</td>
<td>Page 1</td>
<td>55f85f29f66582f6380df9f8b0d4b7d0071bee5fa72958f7817b444c0d8bd</td>
</tr>
</tbody>
</table>
Audit Logistic

- Ensure that adequate space is available for the audit team.
  - Two rooms for the audit team
  - No video conferencing capability (or at least disabled)

- Avoid side conversations

- Redact Sensitive Personnel Information in PRA

- Avoid excessive redaction

- Provide evidence in electronic form (and hard copy if requested)

- Submit all evidence prior to Exit Presentation
Compliance Audit

• Post-Audit Process:
  – RE Management and Enforcement review
  – Draft audit report
  – Entity comments
  – Feedback forms
  – Final audit report (non-public and public versions)
CIP Compliance Workshop

- Wednesday, May 11: 1:00pm – 5:00pm
- Thursday, May 12: 8:00am – 3:00pm
- Registration link: http://www.spp.org/event_register2.asp?oID=3276
- Location: Hilton DFW Lakes
  Grapevine, TX
Questions?
SPP RE CIP Compliance Monitoring Team

Kevin Perry
Director, Critical Infrastructure Protection
kperry@spp.org  (501) 614-3251

Shon Austin
Senior Compliance Specialist – CIP
saustin@spp.org  (501) 614-3273

Leesa Oakes
Compliance Specialist II – CIP
loakes@spp.org  (501) 614-3274