NERC CIP Compliance Audit Lessons Learned

Eric Ervin

SPP CIP Working Group

June 26, 2012
Agenda

- CIP Audit Team Composition
- Audit Preparation
- Audit Timeline
- Onsite Audit
- Lessons Learned & Recommendations
- Questions
CIP Audit Team Composition

Westar’s Audit Team

- Executive Management (7)
- Regulatory Affairs (3)
- Corporate Compliance and Internal Audit (3)
- Corporate and Operational Area SMEs (18)
  - Corporate IT / IT Security
  - EMS
  - Physical Security
  - Substation
  - Generation
- Legal (1)
Audit Preparation

October 2011 3rd-Party Gap Assessment + January 2012 Annual CVA + February 2012 3rd-Party Mock Audit = May 2012 SPP CIP Audit

Assistance Performed By:
- 3rd-Party Consultants
  - Gap Assessment
  - Mock Audit
- Westar’s Internal Audit
  - Testing of High-Risk Requirements
Audit Timeline

- **February 3rd** – CIP Compliance Audit Notice Letter
  - RSAW Development
  - Sample Matrix

- **February 17th** – Submitted Sample Matrix
  - Received Random Sample Selection on February 24th

- **March 9th** – Submitted Evidence Request #1
  - Completed Compliance Pre-Audit Survey
  - Completed RSAWs
  - Evidence Request and Inventory Workbooks

- **April 13th** – Submitted Evidence Request #2
  - 56 Pre-Audit Data Requests
  - Updated Inventory Workbooks
Onsite Audit

- May 7th – 18th
  - 2 Consecutive Weeks (1st week M-F, 2nd week Tu-F)
- 6 SPP Representatives, 3 FERC Observers, No NERC Reps
- “Culture of Compliance” Discussion with Senior Mgmt.
- Initial Scope - 39 of 43 Requirements
- Reviewed Open TFEs and Open Self-Reports
- Physical Inspections
  - Primary and Backup Control Centers
  - Primary and Backup Data Centers
  - Central Monitoring Station
  - Substation
Lessons Learned & Recommendations

Audit Interaction

- Executive and Audit Involvement Key
  - Senior Management, Compliance Officer, IA
- Candid and Open Discussion with Audit Team
  - Willingness to discuss areas of weakness openly.
- Well Prepared SMEs and Supporting Evidence
- Open to Suggestions and Recommendations
- Stressed Westar Energy’s Continuous Improvement
- Timely Data Request Responses (112 Total, 56 Onsite)
  - Majority satisfied within a day.
  - Single Point-of-Contact
Lessons Learned & Recommendations

Overall

- Perform Mock Audit at least 120-days prior to Audit.
- Conduct a facilities tour prep-session.
- Utilize SharePoint (or Doc Mgmt. System) to track and capture document versions.
- Make use of a blog to capture notable observations and lessons learned during the Audit.
- Allow sufficient time and resources to organize the data responses into folder, update the evidence workbooks, and hash (fsumFrontEnd).
- Team lead kicked off discussion, SMEs then provided process details (demonstrated buy-in).
Lessons Learned & Recommendations

**CIP-002**

- CCA List to include the following attributes: CA Supported, PSP Location, ESP Location, Cyber Asset Type, Cyber Asset Function, Host (Machine) Name, Asset Description, Manufacturer, Model, Serial #, Platform/OS, Connectivity, Install Date, Custodian

**CIP-003**

- Information Protection and Access Control Program
  - One program addressing R4 and R5.
  - Information stored and tracked by repository.
  - Moving from multiple directory shares to single NERC CIP repository.
Lessons Learned & Recommendations

CIP-005

- Discovery of Access Points
  - Look at configured interfaces.
- Access points to the ESP include where serial protocols enter into the ESP.
- Findings documented in the CVA will be scrutinized.

CIP-006

- Consider adding “escort transfer” language into the Visitor Control Program.
- Several questions around windows in the PSPs
  - Floor level, wire mesh, tamper monitoring, open?
Lessons Learned & Recommendations

CIP-007

- **Ports and Services**
  - Scan using “netstat -anbo” or Nessus equivalent.
  - Ensure a business justification is listed per service.
  - Document discrepancies (change in baseline) in change management records.

- **Antivirus and Malware Prevention**
  - Consider “burn-in” period in development/test environment.

- **Security Status Monitoring**
  - Provisions must be made to manually review logs for the duration of an outage (monitoring system).
Lessons Learned & Recommendations

CDF-008
- Incident Response Plan
  - If vendors manuals are referenced, document location.
  - Have hard copies available to staff.
- CIP-009
  - Enhance Recovery Plan to include step-by-step instructions for “day-1” employee.
  - Have hardcopies available to staff.
Questions?

Eric Ervin
Westar Energy
Manager, NERC CIP

Eric.Ervin@westarenergy.com

(785) 575-1626