Changes since video was filmed...

- Slide 8 - PRC-001 RSAW Compliance assessment approach has been revised but context of slide is still valid
- Slide 9 - EOP-009 was retired 7/1/13 but context of slide is still valid
- Slide 13 - Exception Reporting was discontinued as a compliance discovery method effective 7/1/13
- Slides 14 & 15 - CANs are in the process of being migrated to the RSAWs

December 2013
Top 10 Ways to Successfully Prepare for an Audit

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

Jeff Rooker
Lead Compliance Engineer
jrooker.re@spp.org 501.614.3278
Audit Prep Outline

• Compliance is an ongoing process
• Ensure evidence is relevant, valid, and reliable
• Be organized
• Self-assess
• Registered Entity is responsible for compliance
• Stay informed, get involved
• Consider outside consultants
• Resources
1. Compliance is an ongoing process

- Get support from the top-down
- Conduct continual review of documentation and procedures
- Documentation of evidence
  - Maintain version history
  - Review documentation annually
  - Ensure process changes are addressed in documentation updates
  - Ensure evidence is relevant, valid, and reliable
2. Ensure documented procedures are relevant

- Issue of procedures created for auditors vs. day-to-day operations use
- Communicate changes in procedures and ensure operational staff are properly trained
3. Examples of Evidence

- Operator logs
- Voice recordings
- Emails
- Screenshots
- Policies/Procedures
- Training attendance lists
- Test results
- Physical and electronic access lists
- Critical Cyber Asset lists
4. What evidence will you need?

- Compliance Assessment approach in RSAW
- Review measures in Standard
- Evidence request and inventory workbook (CIP requirements)
  - Record of submitted evidence
  - Initial evidence requested section
  - Evidence to be randomly sampled section
Review Compliance Assessment Approach in RSAW (PRC-001-1 R1)

Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.

This section must be completed by the Compliance Enforcement Authority.

Compliance Assessment Approach Specific to PRC-001-1 R1.

___ Verify the operator is familiar with relay protection schemes deployed on its system via one of the following:

___ Operator training records indicating training in basic relaying, including any Special Protection Systems within its system.

___ Interview operator(s) to ensure basic knowledge of relaying, including any Special Protection Systems within its system.
Example of Measures in Standard (EOP-009-0 R2)

R2 The Generator Owner or Generator Operator shall provide documentation of the test results of the startup and operation of each blackstart generating unit to the Regional Reliability Organizations and upon request to NERC.

M1 The Generator Operator shall have evidence it provided the test results specified in Reliability Standard EOP-009-0R1 as specified in Reliability Standard EOP-009-0_R2.
## Evidence Request and Inventory Workbook (CIP)

**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>1be4c877477c4d41bf05023dbdf241974be0f25c131ecc715fb8c588e875b49</td>
</tr>
</tbody>
</table>

**Link to workbooks on SPP.org** (see annual folders on left)
5. RSAW narrative should explain how you are compliant

- Consider linking evidence file name in narrative to document in pdf format
- Complete RSAWs for all applicable requirements based on registration and hold for internal use in case audit scope is expanded

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

Acme Power Company has developed a “Voltage and Reactive Plan” as a policy document (Voltage and Reactive Plan.pdf) to address controlling voltage and MVAR flows on its system. This policy is reviewed on an annual basis at a minimum.

Acme Power Company shares its voltage control policies with neighboring Transmission Operators as part of its annual emergency plan distribution process as noted in the example “email receipt of notification to adjacent TOP” for 2008 through 2011.

Acme Power Company monitors key locations and controls reactive devices via SCADA for
6. Be organized

• Assign compliance responsibilities to specific people
  – Testing, Training, HR, Vegetation Management, etc.
• Track compliance tasks and internal controls
  – Outlook, Excel, Lotus Notes, SharePoint
• Use checklists for documentation reviews
  – Assign reviews to specific subject matter experts
    ▪ EMS, Physical Security, Operations, Engineering, etc.
  – Timing (quarterly, annual, etc.)
• Know where documentation is stored
7. Self-assess compliance using discovery methods

- Self-Certifications
- Periodic Data Submittals
- Exception Reporting
- Self-Report when non-compliance is found
  - Shows good culture of compliance
  - Strongly encouraged

- SPP RE and NERC
  - RE Newsletter
  - NERC newsletter – Standards newsletter
  - NERC webinars
  - SPP RE webinars/workshops

- Working groups (CIPWG)

- Standards Drafting Teams

- RTO Compliance Dept. services
  - Compliance readiness reviews, members’ website, etc.

- Know who to contact and utilize appropriate personnel

- Read Compliance Application Notices (CANs)

- Industry conferences
Example: CAN-0043 PRC-005 Protection System Maintenance and Testing Evidence

“CEAs are to obtain evidence that failure or malfunction of a continuously monitored Protection System device produces an alarm and that corrective action will be taken by appropriate parties upon the alarm sounding or being issued. Examples of evidence of alarming include items include, but are not limited to: screen shots of the Supervisory Control and Data Acquisition (SCADA) system depicting Protection System device status, evidence of associated communications, and documentation of corrective action procedures to be taken when an alarm is received. “
9. Registered Entity is responsible for compliance

- Be prepared to explain work performed by third-party on your organization’s behalf
  - For example - MOD and TPL standards (SPP RTO)
  - Be familiar with studies used to identify critical assets
10. Consider using outside consultants

- Define, improve technical processes
- Assist with regulatory approaches
- Provide pre-audit reviews and support for compliance programs and supplement available resources
- Be sure to check out the consultant
  - Call references
- Mock audits
- NERC list of consultants
Summary

✓ Compliance is a continual process
✓ Demonstrate evidence of compliance
✓ Organize documentation, be prepared
✓ Use best practices such as:
  – Completing RSAWS for all requirements
  – Reviewing Compliance Assessment Approaches
✓ Ensure culture of compliance throughout organization
✓ Remain connected to NERC, SPP RE, SPP RTO