

FERC Reliability Audit Docket PA12-17

TIPSC

Jenifur Rancourt

Acting FERC Compliance Program Manager

June 4, 2013



Timeline

- 2011
 - Audit commenced: November
- 2012
 - Data requests began: January
 - On-site interviews & tours: April
 - Follow-up calls and data requests: summer
- 2013
 - Draft report: March
 - Final report: April
 - Implementation plan submitted: May

Process

- Very different from a NERC/regional compliance audit
- Few process documents
- Many requests not linked directly to a NERC standard
- Far-reaching subject matter
- Reliability, compliance, and internal program topics

Process

- Differences from regional audits:
 - Data requests focused on writing new documents
 - Dialogs rather than interviews
 - Presentations requested by SMEs
 - Allowed to ask auditors questions
 - Immediate feedback, suggestions from auditors

Process

- Special challenges
 - Do not destroy order
 - Continuing obligation to respond
 - Audit period started 6/18/2007

Sample FERC Data Request

- Recovery Plans
 - Describe what methods BPA uses to exercise its recovery plans annually.
 - Describe how BPA updates its recovery plan(s) when significant changes to CCAs, based on the BPA change and configuration management process, occur.

Outcomes

- Very collaborative relationship
- Positive verbal feedback on areas BPA is doing well
 - Absent from “exception report”
- Verbal guidance on things BPA could do better
- Written recommendations on areas that could improve compliance
- Two referrals to region for investigation

Implementation Plan

- BPA agreed with 16 recommendations
- Submitted a required implementation plan 30 days after report published
- Quarterly updates until each recommendation is addressed
- Copies of policies and procedures created

Implementation Plan

- Corrective actions and final completion date
- Some tied to existing mitigation plans and projects
- Some actions were completed before the audit closed

Implementation Plan

- Maintenance
 - Improve documentation of intervals
 - Change deviation policy
 - Improve process for entering new equipment into tracking system
- Coordination
 - Include more neighboring entity info into outage planning process
 - More load drop tools & drills

Implementation Plan

- Planning
 - More frequent detailed transmission planning studies
- Critical Asset Identification
 - Clarify & enhance field Critical Cyber Asset identification procedures