NERC Update
Compliance Enforcement Initiative and ERO Strategic Plan
SERC Compliance Seminar
February 28, 2012
• ERO Enterprise Strategic Plan
• Compliance Enforcement Initiative Overview
• FFT Overview
• Examples of filed FFTs
ERO Enterprise Strategic Plan

- Four Pillars of Success

- Strategic Goals
Four Pillars of Success

- Reliability
- Assurance
- Learning
- Risk-Based Approach
• Standards and Compliance
  - Effective Standards through Efficient Processes
  - Strong and Fair Enforcement
  - Promote Culture of Compliance
• Risks to Reliability

  ▪ Identify the most significant risks to reliability.

  ▪ Be accountable for mitigating reliability risks.

  ▪ Promote a culture of reliability excellence.
• Coordination and Collaboration

- Improve transparency, consistency, quality and timeliness of results.
- Operate as a collaborative enterprise.
- Improve efficiencies and cost effectiveness.
Compliance Enforcement Initiative

- Refocus efforts on reliability excellence.
- Eliminate undue regulatory burdens.
- Streamline paperwork and filing requirements.
- Encourage continued timely and thorough self-reporting and mitigation.
- Improve caseload processing.
• Five filings submitted to FERC from September, 2011 to January, 2012.
• Six-month and one-year status reports due to FERC in 2012.
• All eight Regional Entities using new formats.
• NERC is continuing outreach efforts to ensure successful implementation.
Possible Enforcement Tracks

- Dismissal
- Find, Fix, Track and Report (FFT)
- Notice of Penalty (NOP)
• A registered entity may opt out of FFT processing.
• Upon correction and submittal of FFT filing, the Possible Violation (PV) becomes a Remediated Issue.
  ▪ No penalty or sanction is assigned.
  ▪ Formal Mitigation Plans will not be required.
  ▪ Mitigating activity completion may be verified anytime.
• Remediated Issues become part of a registered entity’s compliance history.
  • Remediated Issues may not be contested in subsequent enforcement actions.
FFTs by Month
(September 2011 - January 2012)
Number of FFTs filed at FERC by Regional Entity (September 2011 - January 2012)

- FRCC: 78
- MRO: 68
- NPCC: 13
- RFC: 77
- SERC: 30
- SPP RE: 43
- TRE: 37
- WECC: 17
Number of FFTs by Reliability Standard Family
(September 2011 - January 2012)
FFT Standard Breakdown
(September 2011 - January 2012)

*Chart includes all version of the Standard
Total FFTS/NOPs by Region
(September 2011- January 2012)
Data and Trends

FFTs by Discovery Method as of 1/31/2012

- Internally Identified (Self reports, Self certifications, Data Submittal, Exception reporting)
- Externally Identified (Audits, Spot checks, Investigations)
Evaluation Guidance for FFTs

• Lesser risk (minimal to moderate) to the reliability of the bulk power system (BPS).
• Does not include serious risk issues.
• Existing caseload and new PVs eligible.
• Mitigation completed before filing.
• Repeat violations eligible for consideration depending on circumstances.
**Issue**: For six hours, the Automatic Generation Control was operated in Constant Frequency mode rather than Tie Line Bias mode; discovered through Self-Report.

**Risk**: The improper mode did not result in undue deviation in the system frequency, which was being monitored by the entity's EMS operators.

**Mitigation**: Revised procedures for displaying ACE and controlling ACE during AGC switching.
CIP-001

**Issue:** Emergency Response Plan did not explicitly provide for sabotage response guidelines; found at audit.

**Risk:** Informal procedures existed, and entity does not own any BES elements.

**Mitigation:** Updated current procedure and retrained all personnel.
CIP-002

**Issue:** The entity’s risk-based assessment methodology (RBAM) was not in effect by the compliance date; discovered through Self-Report.

**Risk:** Entity used its own RBAM and determined it owned no Critical Assets that could impact BPS reliability.

**Mitigation:** Created an RBAM and Critical Assets list.
CIP-003

**Issue:** Did not properly document an exception to the Cyber Security Policy; discovered through Self-Report after notice of an Audit.

**Risk:** The entity’s policy required more frequent checks than required by the Standard, and monthly checks were completed before the annual check would have been due.

**Mitigation:** Exception document completed and approved, additional awareness education, and revised process documents for exceptions.
CIP-004

**Issue:** Personnel Risk Assessment (PRAs) not completed within 30 days of granting access to CCAs; found at spot check.

**Risk:** Delays only ranged from one to five days; affected individuals were long-standing employees who had received background checks on hiring.

**Mitigation:** Entity completed the PRAs and addressed gaps in its PRA program.
CIP-005

**Issue:** Failure to identify certain devices as access points to the Electronic Sector Perimeter (ESP); found at audit.

**Risk:** Despite not being labeled as an access point, the device was afforded the required protections.

**Mitigation:** Entity revised its topology diagrams during the audit to include the device as an access point to the ESP.
CIP-006

**Issue:** Entity failed to include all Critical Assets located within an ESP within the six-wall border of a Physical Security Perimeter (PSP); found at Spot Check.

**Risk:** Multiple layers of physical security protected access to the PSP.

**Mitigation:** Entity secured the six-wall border of the PSP before conclusion of the spot check.
CIP-007

**Issue:** Entity did not have a patch management procedure in place and updates were not documented; discovered through Self-Report.

**Risk:** Patches *were* performed informally using an application to identify vulnerabilities in third-party applications.

**Mitigation:** Ticket tracking system put in place and documented; all devices and updates now tracked and documented.
EOP-008

**Issue:** No evidence that it had updated or reviewed its transmission system’s Emergency Operation Plans; discovered from Self-Report.

**Risk:** Entity had a document that acted as its plan for a loss of control center functionality; no substantial changes were made.

**Mitigation:** Entity implemented a mechanism to remind personnel of update cycle; developed and implemented new document review procedure.
FAC-008

**Issue:** Entity did not consider relay protective devices or instrument transformers in Facilities Rating Methodology; found at Audit.

**Risk:** Missing elements were not most limiting elements in design of entity’s generating facility.

**Mitigation:** Entity revised FRM to include missing elements and assigned them ratings according to original equipment manufacturer ratings.
PRC-001

**Issue:** Substation tech disabled primary and backup relaying on a 345 kV line in the adjacent panel when drilling without notifying its TOP; discovered through Self-Report.

**Risk:** Relaying was disabled four minutes prior to notifying the registered TOP, but high-speed clearing of the fault still would have occurred.

**Mitigation:** Operating personnel were retrained on proper notification procedures.
Issue: Entity could not provide basis for maintenance and testing intervals for Protection System devices; found at Audit.

Risk: Entity did have intervals in the program, but only failed to document the basis; performed testing in accordance with the intervals.

Mitigation: Entity added the basis for its maintenance and testing intervals to its program.
PRC-005

**Issue:** Entity missed quarterly interval for battery testing on one battery by 12 days because of broken equipment; found at audit.

**Risk:** Affected 1 of 251 batteries; met monthly and annual testing intervals, as well as quarterly intervals for all other batteries.

**Mitigation:** Entity tested the missing battery, trained on importance of scheduled testing, and modified testing program to include flexibility for short delays caused by extenuating circumstances.
Issue: Of 68 total UFLS devices, 10 devices, approximately 15%, did not have evidence of testing; discovered through Self-Report.

Risk: The entity's identified UFLS equipment only had a possible 80 MW impact for load shed. Upon completing the maintenance and testing, the entity's UFLS equipment performed as expected.

Mitigation: Performed inventory and identified deficiencies, developed a "catch-up" maintenance and testing plan and schedule, trained technicians on the procedures, and completed the required "catch-up."
VAR-002

**Issue:** Operator mistakenly placed a voltage regulator into automatic VAR mode rather than automatic voltage control mode (unclear control panel); discovered through Self-Report.

**Risk:** Corrected promptly, all voltage schedules met; voltage support to BPS continued (to a lesser degree); capacity of fewer than 100 MW and interconnects at lower voltage; and generator not called on to support transmission system voltage.

**Mitigation:** Control panel screen modified; retrained operators on requirements for automatic voltage regulation and operation of the generator control panel.
Some FFT Attributes

- Self-identified issues
- Lesser risk to Bulk Electric System (BES) Elements
- Informal/automatic procedures existed
- Very few devices excluded
- Operated within good utility practice
- Short duration/promptly corrected
- Backup protection/process in place
- Trusted/experienced employee
- No event occurred during violation period
Potential Benefits

• Provides incentive to find and fix issues more quickly.
• Focuses resources on more serious risks to reliability of the BPS.
• Improves alignment of time, resources and record development with the risk posed to reliability.
• Achieves efficiency gains.
• Reduces information dissemination delays.
• Focuses more time on ensuring reliable operations.
Misconceptions Corrected

- Not just older cases
- Not just documentation-only violations
- Not just the *least* risk PVs
- All PVs of a given standard do not qualify for FFT.
- There will be consistency in due process, even if outcomes are not identical.
Implementation Challenges

• Ensuring consistency in evaluation and disposition.
• Addressing pre-existing and repeat violations.
• Determining risk posed to BPS reliability.
• Considering registered entities’ request for FFT treatment.
• Developing information technology (IT) solutions and revised Self-Report Form.
• Uncertainty discourages some entities from participating.
• Training compliance staff to make decisions in the field will be a significant focus in 2012.
• Phase II implementation is currently targeted in 2013.
Potential Improvements

• In Phase II:
  ▪ Continue to alleviate extensive record development burden for lesser risk violations.
  ▪ Provide guidance through FFT candidate examples.
  ▪ Enable compliance staff to identify FFTs.
  ▪ Reap benefits for all.

• Beyond Phase II
  ▪ Aggregated reporting of Remediated Issues.
• Report to be submitted on March 30, 2012.
• Opportunities provided for input by Registered Entities and Regional Entities.
• Experience over first six months to be evaluated.
Tools and training available to Registered Entities and to Regional Entities

- Compliance Workshops
- Compliance Open Webinars
- Certification Programs
Resources and Seminars

• Conveying lessons and changing behavior from Enforcement
  - Notices of Penalty
  - FFTs
  - Best Practices
  - Lessons Learned
  - Dismissal Analysis
  - Case Notes
Conclusion

- Focused strategy
- Outreach on all fronts

We are all accountable for ensuring reliability.