NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CEI Webinar

Find, Fix, Track and Report (FFT) Update

February 2, 2012

RELIABILITY | ACCOUNTABILITY




Agenda

1) Purpose of CEI and overview of FFT
2) Implementation of FFT to date
3) Preparation for 6-month filing with FERC
4) Timeline for phased implementation
5) Discussion of specific FFT Remediated Issues

Purpose

- Refocus efforts on reliability excellence
  - Differentiate issues of noncompliance based on the level of risk to the reliability of the bulk power system
  - Continue to identify, correct and report all instances of noncompliance
- Eliminate undue regulatory burdens
- Streamline paperwork and filing requirements
- Encourage continued timely and thorough self-reporting and mitigation
- Improve caseload processing

Overview of FFT

- A Registered Entity may opt out of FFT processing
- Upon correction and submittal of FFT filing, the Possible Violation 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

Initial CEI Filing

- On September 30, 2011, NERC filed several components of the Compliance Enforcement Initiative
  - Petition for Approval of New Enforcement Mechanisms
    - Reports due to industry at six months and one year
  - 117 FFT Remediated Issues
  - 75 Spreadsheet NOPs
  - 27 Full NOPs
- On October 28, 2011, FERC issued notice of no further review of the Spreadsheet NOPs and the Full NOPs

Second CEI Filing

- On October 31, 2011, NERC filed the second group
  - 82 FFT Remediated Issues
  - 46 Spreadsheet NOPs
  - 31 Full NOPs
- On November 30, 2011, FERC issued notice of no further review of the Spreadsheet NOPs and the Full NOPs

Third CEI Filing

- On November 30, 2011, NERC filed the third group
  - 50 FFT Remediated Issues
  - 60 Spreadsheet NOPs
  - 21 Full NOPs
- On December 30, 2011, FERC issued notice of no further review of the Spreadsheet NOPs and the Full NOPs

Fourth CEI Filing

- On December 30, 2011, NERC filed the fourth group
  - 76 FFT Remediated Issues
  - 54 Spreadsheet NOPs
  - 15 Full CIP NOPs
- On January 27, 2012, FERC issued notice of no further review of the Spreadsheet NOPs and the Full NOPs

Fifth CEI Filing

- On January 31, 2012, NERC filed the fifth group
  - 57 FFT Remediated Issues
  - 51 Spreadsheet NOPs
  - 21 Full CIP NOPs
- FERC order pending

FFTs by Regional Entities

- FRCC 77
- MRO 68
- NPCC 13
- RFC 77
- SERC 30
- SPP RE 43
- TRE 37
- WECC 17

FFTs by Family

- CIP 234 (62 TFEs)
- PRC 40
- FAC 36
- EOP 25
- VAR 14
- TOP 7
- BAL 6
- PER 6
- MOD 3
- TPL 3
- COM 3
- INT 2
- IRO 2
- NUC 0

CEI Reports to FERC

- NERC committed to submit six-month and one-year informational filings with FERC
  - On or about March 30, 2012
  - On or about September 28, 2012
- NERC is working with Regional Entities
- NERC is soliciting Registered Entity feedback
  - February MRC meeting
  - Registered Entity responses to survey were due February 1, 2012
  - Written comments may be submitted by e-mail on or before February 23, 2012

6-Month Status Report to FERC

- Guidelines
- Data and Trends
- Benefits
- Implementation and Transition Challenges
- Potential Improvements
- Training Schedule

Timeline

Phase I – September 2011

Possible Violations identified in all compliance monitoring methods qualify for FFT Report consideration

Phase II – September 2012 or later

CEA auditors make determinations in the field on disposition tracks; CEA Enforcement staff make determinations on other monitoring methods

Phase III – 2013 or later

Future options could include aggregated reporting of Remediated Issues to CEA, NERC and FERC

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Specific FFT Remediated Issues

Issues, Risk and Mitigation

RELIABILITY | ACCOUNTABILITY




Summary

- To date, 382 FFTs filed
  - They include minimal to moderate risk issues
  - They include documentation and operational issues
  - 1 was moved to Spreadsheet NOP
- Of these, 61 were late-filed TFEs
  - 50 were CIP-007
  - 7 were CIP-005
  - 4 were CIP-006

Online Resources

- This presentation provides a high level summary of some FFT remediated issues. For further details on individual FFTs filed with FERC as of January 31, 2012, please refer to the searchable FFT spreadsheet, available at :

  http://www.nerc.com/filez/enforcement/index.html

- For a complete set of NERC-approved mandatory Reliability Standards, please refer to:

  http://www.nerc.com/page.php?cid=2|20

BAL-003-0.1b

Issue	Risk	Mitigation
R2: Fixed Frequency Bias	Minimal: Bias setting used single most severe disturbance to determine Frequency Bias rather than averaging several	Revise procedure to ensure several disturbances used
R3: AGC Settings	Minimal: EMS was continuously monitored, issue occurred during minimal usage period, no deviation in system frequency	Update cyber security change control protocols

BAL-005-0.1b

Issue	Risk	Mitigation
R11: Ramp Rates	Minimal: Impact was increase in inadvertent energy during ramp times	Update procedures for e-tag review and approval
R6: AGC Mode	Minimal: AGC mode has little impact to system frequency deviations, system frequency was monitored	Update cyber security change control protocols
R8: RTU Scan Rate	Minimal: Limited # scan rates and longer scan rate than minimum	Change scan rates and updated data acquisition procedure

CIP-001-1

Issue	Risk	Mitigation
R1: Sabotage Awareness Procedures	Minimal: Little or no BES facilities; relied on third party process; security policy	Adopt procedure addressing sabotage
R2: Sabotage Communication Procedures	Minimal: Little or no Critical Assets, Critical Cyber Assets or BES facilities	Adopt procedure or include language on sabotage reporting
R3: Sabotage Guidelines for personnel	Minimal: Little or no Critical Assets, Critical Cyber Assets or BES facilities	Adopt and disseminate procedure or include language on sabotage reporting
R4: Contact FBI on sabotage events	Minimal: Little or no Critical Assets, Critical Cyber Assets or BES facilities	Adopt procedure to contact FBI for sabotage

CIP-001-1a

Issue	Risk	Mitigation
R1: Communicating sabotage events to personnel	Minimal: Personnel trained on sabotage and list of local authorities contact info maintained on site	Adopt procedure to increase awareness of personnel
R2: Communicating sabotage events to other entities	Minimal: Personnel trained on sabotage and list of neighboring entities contact info maintained on site	Adopt procedure to recognize and report sabotage events
R3: Communicating sabotage to law enforcement	Minimal: Little or no Critical Assets, Critical Cyber Assets or BES facilities	Adopt procedure to recognize and report sabotage events

CIP-002-1

Issue	Risk	Mitigation
R1: Risk based assessment methodology	Minimal: No CAs that could impact the BPS, size of entity	Adopt appropriate methodology and implement
R2: Failure to identify all cyber assets in methodology	Minimal/Moderate: No CAs, CCAs on system or minimal delay in identification	Correct misidentification of assets and develop accurate list
R3: Develop list of all critical cyber assets (CCA)	Minimal: Assets incorrectly identified as CCAs or omitted but did not leave assets unprotected	Correct misidentification of assets and develop accurate list
R4: Review and approve the list of CCAs annually	Minimal: No CCAs identified or minimal delay in developing initial list	Establish procedure to document status of CCAs and approve annually

CIP-002-2

Issue	Risk	Mitigation
R1: Risk based assessment methodology: omission of evaluation criteria	Minimal: Entities did correctly evaluate assets using studies	Adopt appropriate methodology and implement
R3: Develop list of all critical cyber assets (CCA)	Minimal: Assets incorrectly identified as CCAs and added to list	Correct misidentification of assets and develop accurate list
R4: Review and approve the list of CCAs annually	Minimal: No CAs or CCAs identified or minimal delay in developing initial list; no senior manager signed and dated record of approval	Establish procedure to document status of CCAs and approve annually

CIP-002-3

Issue	Risk	Mitigation
R1: Risk based assessment methodology: third parties	Minimal: Third party assets were not considered; communications could not directly control assets	Amend procedure to include review of third parties
R2: Develop list of all critical cyber assets (CCA)	Minimal: No CAs and CCAs identified for entity involved	Adopt procedure to review annually
R3: Review and approve the list of CCAs annually	Minimal: No CAs and CCAs identified for entity involved	Adopt procedure to document status of CCAs and approve annually
R4: Review and approve CCA Methodology annually	Minimal: Approved its RBAM in the previous and following years	Adopt procedure to review methodology and approve annually

CIP-003-1

Issue	Risk	Mitigation
R1: Cyber Security Policy	Minimal/Moderate: Policies in place but documentation inconsistencies	Revise CSP to comply with requirements of standard
R2: Senior manager responsibility for CIP	Minimal: No or minimal CCAs identified for entities involved/documentation error	Assign senior manager responsibility and document
R3: Exceptions to cyber policy	Minimal: Third parties preparing compliance with CIP Standards; gap in compliance	Adopt procedure to address exception reporting
R4: Information Protection	Minimal: Mislabeled information related to CCAs	Reviewed all related information and corrected deficiencies.
R6: Change Control for CCAs	Minimal: Had a non-documented process to track changes	Document change related to control process

CIP-003-3

Issue	Risk	Mitigation
R2: Senior manager responsibility for CIP	Minimal: Documentation issues with updating personnel changes due to turnover, no gap in Compliance	Modified procedures, documented the personnel with CIP accountability

CIP-004-1, -2 and -3

Issue	Risk	Mitigation
R2: Cyber security training programs	Minimal: Contractors and internal personnel were not given CIP training prior to access to CCAs	Training for personnel granting access enhanced and tracking of personnel with access implemented. Automatic revocation of access if not trained
R3: Personnel assessment for all with access to CCAs	Minimal: Involved long-time employees/contractors	Audited personnel records and performed required PRAs; verified third parties performed and provided PRAs
R4: Unescorted access to CCAs: changes	Vendor/Contactor lists were not reviewed quarterly but annually in most cases; physical access devices were taken upon employment status changes	Develop improved tracking process to track vendor updates and personnel status changes

CIP-005-1 and -3

Issue	Risk	Mitigation
R1: Cyber assets within the Electronic Security Perimeter	Minimal: Unidentified assets were used to monitor network traffic	Updated training on how to identify CCAs and updated network topology correctly
R3: Monitoring electronic access; documentation	Minimal: review and logging process not properly documented	Document logging processes and publish appropriately

CIP-006-1, -2 and -3c

Issue	Risk	Mitigation
R1: Physical security plans and access controls; CCAs	Minimal: Facilities monitored electronically 24/7 and access was limited	Physical issues were addressed with barriers; enhanced CIP training regarding visitor access inside Physical Security Perimeter(PSP)
R4: Physical access controls; logging visitor access	Minimal: All admitted inside PSP has been trained and approved	Communicate to staff and enhance training on visitor logging
R7: Access logs: retention	Minimal: All controls were in place when logging software was inoperative	System reconfigured to prevent recurrence of error

CIP-007-1, -2, and -3

Issue	Risk	Mitigation
R1: Test procedures; new or significantly changed CCAs	Minimal: Documentation of compatibility with existing CCAs	Additional testing completed and documented.
R2: Ports and services	Minimal: Unnecessary ports and services not open on CCAs	Disabled ports and services on devices
R5: Account Management: passwords	Minimal: Physical security and access to CCAs was maintained and persons with access were properly trained and screened	Upgraded technology and procedures to accurately track access and flag for update as necessary
R6: Security status monitoring: logs	Minimal: Continuous monitoring within the ESP was uninterrupted	Implement procedure to ensure regular security log review

CIP-008-1, -2 and -3

Issue	Risk	Mitigation
R1: Cyber Security Incident Response Plan: Maintaining and updating plans	Minimal: Documentation errors were corrected promptly and measures were in place through other procedures at the organization to ensure compliance.	Correct deficiencies and update plans to require updates that meet the requirements of the Standard.

CIP-009-1, -2

Issue	Risk	Mitigation
R1: Recovery plans for CCAs: Cyber assets included and activation criteria	Minimal: Plans included necessary steps but not activation criteria	Updated plans to include varying activation based on duration and severity level

COM-002-2

Issue	Risk	Mitigation
R2: Three part communication	Minimal: Directives were not repeated back to ensure accuracy during a voltage adjustment event	Additional training to staff involved in issuing and receiving directives was provided.

EOP-001-0 and -1

Issue	Risk	Mitigation
R3: Development and maintenance of plans for emergency situations	Minimal: SCADA included a load reduction schedule all operators were trained to use the system	Plans for load shedding and system restoration were developed and implemented
R4: Communication protocols for emergencies	Minimal: Other company documents outlined procedures	Plans for emergency communication protocols were implemented
R5: Incomplete emergency plan: Attachment 1	Minimal: Entity had all other elements in its plan	Created an emergency plan that incorporated all elements
R6: Emergency plans	Restoration plans were in place but not communicated to neighboring entities	Plans shared with appropriate entities
R7: Coordinating emergency plans	Minimal: Operators had tools in place to communicate	Update communication protocols and procedures

EOP-003-1

Issue	Risk	Mitigation
R8: Lack of load shedding plans for real-time emergencies	Minimal: Other company documents gave operators the authority to shed load during emergencies	A load shedding plan that met the requirements of the Standard was created

EOP-004-1

Issue	Risk	Mitigation
R3: Reporting a reportable incident: 24 hour limit	Minimal: Entities reported these storm related events on a delayed basis (within 4 days) after addressing the root causes and attempting repairs	Procedures were amended to ensure NERC reporting according to the Standard was completed within 24 hours

EOP-005-1

Issue	Risk	Mitigation
R1: System Restoration Plans: Attachment 1 elements	Minimal: Entities demonstrated they could implement the plans	Plans were revised to include missing elements
R4: Coordinating restoration plans	Minimal: Plans were in place and operators trained on them	Plans were communicated to neighboring entities
R6:Restoration plans: training annually	Minimal: Employee lacking training was a 12 year veteran	Operator completed training and plan updated to include annual simulations
R7: Restoration Procedure: actual testing/simulations	Minimal: Documented procedure existed and was used in training	Consultant retained to validate procedure using simulations

EOP-008-0

Issue	Risk	Mitigation
R1: Control Center loss planning: annual tests and updates	Minimal: Plans were missing various components and, in most cases, were being tested annually. Plans that were not being tested and updated annually were in situations where no material changes had occurred	Plans were updated to address missing elements and processes put in place to ensure an annual test and complete review of the existing plans

FAC-001-0

Issue	Risk	Mitigation
R1: Facility connection requirements	Minimal: All applicable sub-requirements would have been discussed during the engineering studies related to an Interconnection	Facility connections requirement procedures were created
R2: Facilities connection document: requirements	Minimal: Requirements were discussed during the interconnection process in all cases	Missing elements were included in the procedure

FAC-003-1

Issue	Risk	Mitigation
R1: Vegetation management program	Minimal: Lacked procedures for immediate communication of imminent threats by vegetation; long vegetation growing times; periodic ground inspections	Revised document to include procedure for communication of vegetation creating an imminent threat

FAC-008-1

Issue	Risk	Mitigation
R1: Facilities rating methodology: not including all requirements	Minimal: Entities operated the equipment according to manufacturer's specification even though the omitted facility ratings for some devices or failed to include required items in their facilities ratings methodology	All entities revised their documents to include information missing from its facility rating methodology

FAC-009-1

Issue	Risk	Mitigation
R1: Facility ratings based on facility ratings methodology: implementation	Minimal: Entities did not include all elements in their methodology, at times the most limiting element, but operated the equipment within manufacturer's design specifications	All entities revised their facility rating methodology documents to include missing devices and established updated facilities ratings

FAC-010-1

Issue	Risk	Mitigation
R1: System Operating Limit(SOL) Methodology	Minimal: Entity involved is small with only a single connection to another Transmission Operator	A SOL methodology was developed and implemented

FAC-014-2

Issue	Risk	Mitigation
R5: Providing SOLs to other entities	Minimal: The SOL affected only the entity and did not have an impact outside of its footprint	The SOL was provided to the necessary entity

INT-006-3

Issue	Risk	Mitigation
R1: On-time request for interchange (RFI) responses	Minimal: Delays averaged only minutes and had an economic impact only on limited RFI transactions	A formal practice for responding to RFIs was developed and staff trained

IRO-004-1

Issue	Risk	Mitigation
R4: Providing information to Reliability Coordinators	Minimal: In one case, the generator was not an available resource to the RC and in the other it was a one-time occurrence mitigated in real-time	Communications protocols were developed and existing protocols enhanced to include verifications

MOD-001-1a

Issue	Risk	Mitigation
R8: Re-calculating Available Transfer Capacity within required timeframes	Minimal: The entity operated its system with an accurate ATC and did recalculate within 16 days of the mandatory timeframe	The ATC was recalculated prior to the planned outage

MOD-019-0

Issue	Risk	Mitigation
R1: Correctly reporting forecasts of interruptible demand and DCLM	Minimal: The data is used for long term forecasting and only one year was reported inaccurately	Require additional review of form EIA-411 before submittal in a written procedure

PER-002-0

Issue	Risk	Mitigation
R1: Adequately staffed with properly trained operating personnel	Minimal: Personnel NERC certified, met required emergency ops training	Added training personnel and completed required course training for operators
R3: Demonstrate competent training staff and program	Minimal/Moderate: Training staff had operational experience but lacked training expertise	Hired vendors or hired personnel with proper training credentials
R4: Cannot demonstrate that other training requirements met	Minimal: Personnel all NERC certified, met required emergency ops training but lacked additional training	Added training personnel and completed required course training for operators

PER-003-0

Issue	Risk	Mitigation
R1: Personnel performing BES related duties were not NERC certified	Minimal/Moderate: Entities were in the process of obtaining NERC certification and only a small percentage were not certified	Entities completed NERC certification process within timeframes allotted

PRC-001-1

Issue	Risk	Mitigation
R3: Protection system changes made without informing neighboring TOPs and BAs	Minimal: Changes actually enhanced reliability but lacked evidence of coordination	Procedure modified to ensure proper communication. TOPs and BAs received new settings
R4: Protection system changes on transmission lines made coordinating with neighbors	Minimal: Changes only affected internal footprint and not neighboring TOPs or BAs	Changes communicated to neighbors. Procedure put in place to ensure future coordination
R5: Protection system on 345kV tie line disabled without notification to neighbors	Minimal: TOP was notified 4 minutes after disabling of protection system	All field technicians retrained on proper notification procedures

PRC-004-1

Issue	Risk	Mitigation
R1: Protection system misoperations: corrective action plans (transmission)	Minimal/Moderate: Not all misoperations were being analyzed and addressed	Procedure now clearly identifies steps in analyzing misoperations and when an action plan is appropriate
R2: Protection system misoperations: corrective action plans (generation)	Minimal/Moderate: Procedures for analyzing and mitigating misoperations were deficient	Procedure now clearly identifies steps in analyzing misoperations and when an action plan is appropriate
R3: Protection system misoperations: reporting	Minimal: While not reported, the misoperation was mitigated and a plan developed	Procedure modified to monitor misoperations and ensure appropriate reporting

PRC-005-1

Issue	Risk	Mitigation
R1: Protection system maintenance and testing: requirements	Minimal: Most devices were tested and, in some cases, devices were tested to manufacturers specs rather than to procedure	Procedures updated to include missing requirements and all devices tested according to procedure within time allotted
R2: Protection system maintenance and testing: documentation of implementation	Minimal: Documentation not available to show all devices tested, only most devices	Testing completed on all devices and tracking procedure updated to ensure testing completed to schedule

PRC-008-0

Issue	Risk	Mitigation
R1: Under frequency load shedding(UFLS): testing and maintenance program	Minimal: maintenance and testing performed but records not available. Entities in question also very small	Created separate UFLS maintenance and testing program document that included record keeping
R2: UFLS: program results	Minimal: Little load at risk due to small size of entities	Established procedures for identifying, maintaining and testing UFLS devices and tested the devices according to program

PRC-023-1

Issue	Risk	Mitigation
R1: Phase protective relay settings: settings	Minimal: only one of fifty-nine relays settings not appropriate, it was an overreaching relay that would have tripped	Recomputed, coordinated and reset relay to appropriate value

TOP-002-2a

Issue	Risk	Mitigation
R3: Coordination of operations	Minimal: One weekend message failed to be transmitted to the appropriate parties	Updated procedure to eliminate communication issues with transmission of reports and retrained operators
R14: Communicating changes/reduction in capabilities due to fuel	Minimal: Actual reduction in capability was minimal and of short duration	Develop document on reportable events for operators and train operators on same

TOP-003-0

Issue	Risk	Mitigation
R1: Planned outages: communication and coordination	Minimal: One weekend message failed to be transmitted to the appropriate parties and another entity had no procedure but also no outages	Updated procedure to eliminate communication issues with transmission of reports and retrained operators

TOP-005-1.1a

Issue	Risk	Mitigation
R1: Automatic voltage regulator(AVR) reporting	Minimal: Entity was aware of lack of AVR and was maintaining voltage manually	A new procedure for AVR status change tracking was developed and operators trained

TOP-006-1

Issue	Risk	Mitigation
R1: Status of resources: communication	Minimal: One weekend message failed to be transmitted to the appropriate parties and another entity had no procedure but also no outages	Updated procedure to eliminate communication issues with transmission of reports and retrained operators

TPL-001-0.1

Issue	Risk	Mitigation
R1: Transmission planning: annual assessment	Minimal: Stability assessment was developed and procedures in place to deal with issues but results not documented, procedure coordinated with the RC	Results documented showing requirements met

TPL-002-0

Issue	Risk	Mitigation
R1: System performance after loss of single BES element	Minimal: Stability assessment was developed and procedures in place to deal with issues but results not documented; procedure coordinated with the RC	Results documented showing requirements met

TPL-003-0

Issue	Risk	Mitigation
R1: System performance after loss of two or more BES element	Minimal: Stability assessment was developed and procedures in place to deal with issues but results not documented; procedure coordinated with the RC	Results documented showing requirements met

VAR-001-1

Issue	Risk	Mitigation
R6: Loss of AVR: communications	Minimal: The TOP was aware of the unavailability of AVR and was regulating voltage manually	A new procedure for AVR status change tracking was developed and operators trained

VAR-002-1

Issue	Risk	Mitigation
R1: AVR mode: communication	Minimal: Voltage support was maintained without the use of AVR on a small unit during the period in question	Modified control panel/system alerts and trained the operators on new displays/alerts and AVR requirements

VAR-002-1, -1.1a and -1.1b

Issue	Risk	Mitigation
R1: AVR mode: communication	Minimal: Voltage support was maintained without the use of AVR during the period in question	Modified control panel/system alerts and trained the operators on new displays/alerts and AVR requirements
R2: Maintaining voltage as directed	Minimal: Entity continued to contribute VARs to the BPA, just in a narrow bandwidth	Worked with Transmission operator to modify load schedule and updated manuals on issue
R3: Status or capability changes: 30 minute notification	Minimal: In most cases, notification was in minutes past the deadline	Reviewed procedures regarding VAR changes and added functionality to monitor VAR settings (for example, alarms)

VAR-002-WECC-1

Issue	Risk	Mitigation
R1: AVR requirement: 98% of the time	Minimal: Only one turbine was not operating in AVR mode bringing the total to 95% for the operator for the period	The entity place the unit back in AVR mode as requested

Questions?

Questions?