October 12, 2012

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose, Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: ***North American Electric Reliability Corporation***
Compliance Filing
Docket No. RC11-6 -___

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby submits this filing in compliance with Paragraph 11 of the Federal Energy Regulatory Commission's (FERC or Commission) September 20 Order.[1] In its September 20 Order, the Commission directed NERC to file the training materials that it developed to facilitate the implementation of Find, Fix, Track and Report (FFT) determinations within thirty days from the issuance of the September 20 Order. This filing contains the following materials which are submitted in compliance with that directive:

- This transmittal letter;
- **Exhibit A -** Compliance Enforcement Initiative Update: The Next Steps for Registered Entities (July 11, 2012) (Washington, D.C.) **–** A PowerPoint presentation used during a NERC webinar

[1] *North American Electric Reliability Corporation*, 140 FERC ¶ 61,215 (2012) (September 20 Order).

for industry stakeholders which focused on new developments under the Compliance Enforcement Initiative (CEI) and provided guidance on self-reports.

- **Exhibit B -** Auditor Training (September 19 – 20, 2012) (Atlanta, GA) – An exercise booklet of sample FFT fact patterns used during breakout sessions with auditors to determine the appropriate processing track.
- **Exhibit C** – Instructors Training (September 19 – 20, 2012) (Atlanta, GA) – An exercise booklet containing the same sample FFT fact patterns as the Auditor Training materials and the answer keys.
- **Exhibit D –** Compliance Enforcement Initiative Training for Auditors and Investigators (September 20, 2012) (Atlanta, GA) – A PowerPoint presentation used to train compliance and enforcement staff on the FFT process.
- **Exhibit E –** Compliance Enforcement Initiative Training for Industry (September 21, 2012) (Atlanta, GA) – A PowerPoint presentation used to train industry members on the FFT process.

NERC respectfully requests that the Commission accept this filing in compliance with the Commission's September 20 Order.

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/ Rebecca J. Michael
Charles A. Berardesco
Senior Vice President and General Counsel
Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters

Exhibit A

Compliance Enforcement Initiative Update: The Next Steps for Registered Entities

July 11, 2012 -- Washington, D.C.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Enforcement Initiative Update: The Next Steps for Registered Entities

Sonia Mendonça, NERC Attorney
Ed Kichline, NERC Manager of Enforcement Processing
July 11, 2012

RELIABILITY | ACCOUNTABILITY




Agenda

- FERC's March 15, 2012 Order
- NERC's May 14, 2012 Status Report and Compliance Filing
- Self-Monitoring and Self-Reporting
- Guidance on Risk Assessments
- One-Year Report on CEI Due March 15, 2013
- Roles of Registered Entities

March 15, 2012 CEI Order

- All six FFT filings submitted to FERC from September, 2011 to February, 2012 were approved in the March 15, 2012 Order.
- Six-month report and compliance filing related to compliance history and further implementation made May 14, 2012.
- One-year report due in March 2013 – Commission will consider changes to the March 15th Order conditions.

Limited Conditions

- Conditions related to eligibility for FFT treatment
  - Prospectively, only Possible Violations that pose a minimal risk are eligible.
  - If an FFT matter is not mitigated as certified, it will be treated as a continuing Possible Violation not eligible for FFT treatment.
- Conditions related to Documentation
  - A registered entity that receives FFT treatment must certify that mitigation is completed.

Limited Conditions

- Condition related to Accountability and Deterrence
  - FFT informational filings must publicly identify the registered entity with a Possible Violation.
    - Exception for CIP violations remains.

Finality

- An FFT matter will be closed 60 days after the FFT informational filing is submitted to FERC.
  - March and April filings now closed.
- FERC will not reopen an FFT for review unless it provides notice that it will review a specific matter.
- Within the 60-day window, FERC expects to exercise review infrequently and in limited and rare circumstances.
  - Insufficient mitigation.
  - Greater than minimal risk.
  - Pattern of non-compliance.

FFT Accountability

- FERC and the ERO will randomly sample FFTs.
- Certification of completion of mitigating activities.
- Unmitigated issues become ineligible for FFT.

Review of Existing Requirements

- FFT may highlight requirements that do little to protect reliability.
  - Removing requirements = Greater compliance efficiency.
- Identification of requirements for revision or removal.
  - Concurrent submittals to FERC.

May 14, 2012 Compliance Filing

- Sustainability and Expandability of the CEI.
- Compliance History as a Factor in Considering FFT Treatment.
- Future CEI Implementation.

Sustainability and Expandability of the CEI

- First step for expansion – to have recommendations from compliance monitoring staff regarding the disposition of certain possible violations as FFTs.
- Ongoing and consistent training:
  - Training and outreach sessions for Regions' enforcement and compliance staff on recommendations for the processing track.
  - Expandability not only in who may recommend potential FFT issues, but also in the effectiveness of the program.
- Goal is to identify minimal risk issues as early as possible.

Compliance History as a Factor in Considering FFT Treatment

- Repeat issues are eligible for FFT provided that the issues pose only a minimal risk to reliability of the BPS.
- Factors include (a) timing of violations/issues, (b) nature of violations/issues, and (c) method of discovery.
- Issues that would NOT be afforded FFT treatment:
  - Where entity's compliance history is indicative of broader concerns.
  - Where prior remediated issue was subsequently found not to have been mitigated.
  - Cases involving material misrepresentations about the nature and scope of the prior issue.

Future CEI Implementation

- Training and Outreach Activities – NERC hosts various workshops and training opportunities for Regions and registered entities. Specific CEI training will be provided to CEA staff on the consistent implementation of the FFT program.
- Coordination and Collaboration – Compliance monitoring staff will make recommendations on the processing track.
- Consistency and Due Process.

Future CEI Implementation

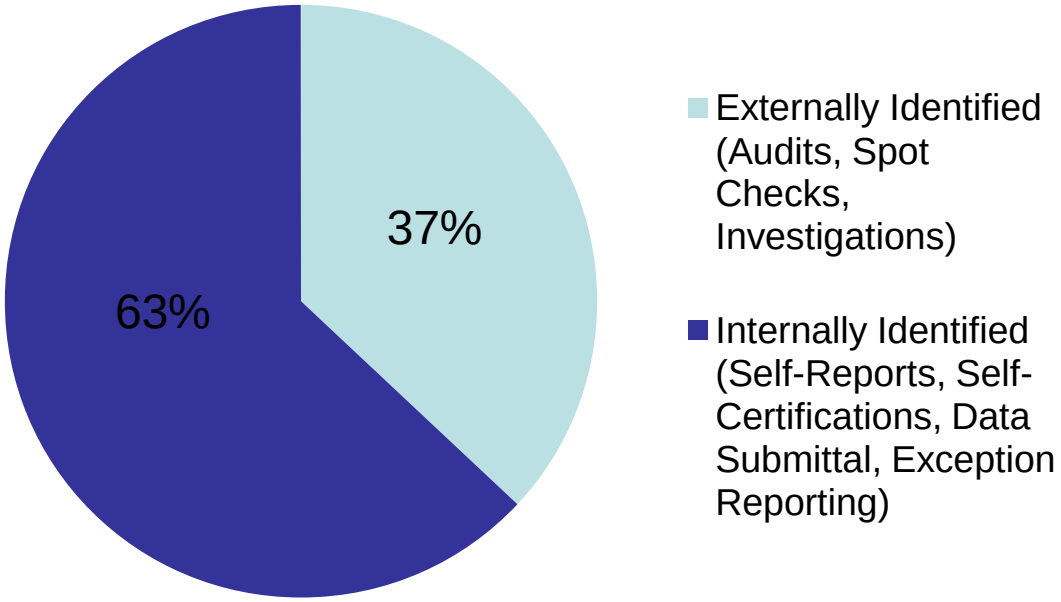
- The Regional Entities and NERC continue to work on plans for improvement of compliance monitoring and enforcement.
- NERC will conduct focus groups with registered entities to solicit feedback and input.
- Submit comments on CEI to ceicomments@nerc.net.
  - Process improvements.
  - Differences between FFT processing and violation processing.

May 14, 2012 Status Report

- Self-Identified Violations Remain Strong.
- Improvement in Processing Efficiencies.
- Standards Receiving the Highest FFT Treatment.
- Next Steps in CEI Implementation.

Self-Identified Violations Remain Strong

FFTs by Discovery Method as of 6/30/12



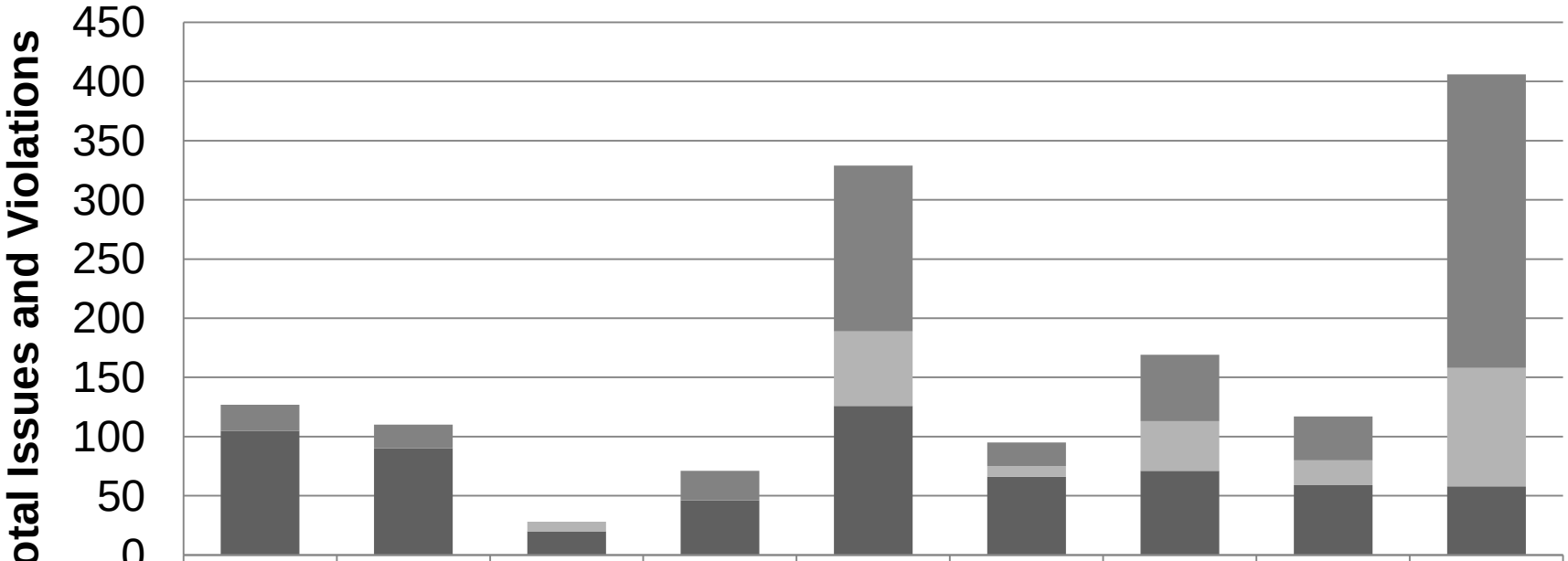
- Incentives:
  - Avoiding a monetary penalty.
  - Abbreviated enforcement process.

FFT Data

- Average duration from discovery to filing:
  - For FFTs discovered after July 1, 2011 = 6.3 months.
  - The ERO is committed to reducing this time.
- Of the 641 FFTs filed, 350 were for CIP-002 through CIP-009 standards violations.
  - 101 of the 350 were CIP-007.
- The highest number of non-CIP FFTs were the 48 CIP-001 issues, followed by 42 PRC-005 issues.

CEI Processing by Region

FFTs/ SNOPs/NOPs
Filed from Sept 2011 to June 30, 2012



	FRC	MRO	NCE	NPC	RFC	SER	SPP	TRE	WEC
SNOP	22	20		25	140	20	56	37	248
NOP	0	0	8	0	63	9	42	21	100
FFT	105	90	20	46	126	66	71	59	58

Next Steps in the CEI Implementation

- Develop a training program for CEA compliance and enforcement staff that will address:
  - Factors to be evaluated when considering processing track.
  - Changes to existing processes that will result from the extension of FFT recommendations by CEA compliance monitoring staff to enforcement staff.
- Public education and outreach activities to evaluate and improve the program will also continue.

Importance of Self-Reports

- NERC's "Guidance for Self Reports" available on its website.
  - Provide complete information early in process.
- FFT should promote better internal reviews and self-reporting.
  - Percentage of self-identified violations should continue to grow.
- Move compliance monitoring responsibilities and decisions on disposition to earlier points.
  - Demonstrable cultures of compliance and internal controls.

Culture of Reliability Excellence

- Expectations for increased compliance as experience with mandatory Reliability Standards grows.
- Serious treatment for violations that should have been self-identified.
  - Less likely to be FFTs.
- The ERO and registered entities must continue to perform in order to exercise additional discretion.

Guidance on Risk Assessment

- No adverse impact ≠ minimal risk.
  - However, other factors may lead to minimal risk.
- Do not base risk assessments on assumptions.
  - Stick to the facts.
- Programmatic shortcomings ≠ minimal risk.

Guidance on Risk Assessments

- Assess risk at the time of the possible violation.
- Existing processes and contemporaneous actions can make actual risk < potential risk.

How to Spot an FFT

- Mostly 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—though not as single factor.

One-Year Filing in March, 2013

- Near final draft anticipated in early February, 2013.
- NERC is working to collect the information required in the one-year report.

One-Year Filing in March, 2013

- FERC will use the filing to evaluate the effectiveness of the FFT program with regard to such matters as:
  - The effect of the program on improving BPS reliability – narrative discussion of risk-based approach and how FFT fits in.
  - The effect of the program on addressing NERC's compliance and enforcement program, including its caseload – graphs similar to 6-month report.
  - The effect of the program on NERC and the Regions better focusing resources on addressing more serious violations – experience dealing with serious issues.

One-Year Filing in March, 2013

- How NERC's evaluation of risk in identifying candidate for possible violations for FFT treatment has evolved, including how VRFs are considered in the evaluation.
- How the FFT mechanism can be improved based on experience – view of end state and desired improvements.
- Results of audits, spot checks or random samplings that NERC or the Regions performed regarding the FFT process – NERC developing a random sampling approach.
- The impact, if any, the implementation of the FFT mechanism has had on the number of Self-Reports submitted – will be tracking level of Self-Reports.

One-Year Filing in March, 2013

- NERC's evaluation of the consistency and application of the FFT initiative:
  - Addressed above re: audits, spot checks, and other sampling methods. The results of those monitoring activities are expected to provide insight into consistency issues.
  - NERC expects to expand on the review and coordination processes currently in place, which have been discussed in prior filings.

What Registered Entities Can Provide

- Effect the FFT process has had on the allocation of resources to compliance activities.
- Ways in which the FFT mechanism can be improved.
- Effects on internal controls and willingness to self-report.
- Experience so far with the Regions on processing FFTs.
- Develop and track efficiency metrics to provide further information on the impact of the program on processes.

Summary

- FERC has provided support and guidance for the CEI.
- NERC and the Regions will continue to work with registered entities on compliance and enforcement efficiencies.
- Registered entities should continue to be on the frontlines of maintaining and ensuring reliability.

Questions?

Sonia Mendonça
Attorney
(202) 644-8046
sonia.mendonca@nerc.net

Ed Kichline
Manager of Enforcement Processing
(202) 400-3025
ed.kichline@nerc.net

Exhibit B

Auditor Training

September 19 – 20, 2012 - Atlanta, GA

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Auditor Training

Atlanta

September 19-20, 2012

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

CIP Examples

Example 1

CIP-007-3 R9

Cyber Security – Systems Security Management

R9. *Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.*

The registered entity failed to document changes made to CIP-007-3 R5 procedure/policy within 30 days, pursuant to CIP-007-3 R9. The department responsible for the support of the network devices in the energy management system (EMS) environment created a process document to capture the procedures and policies for "account management" as specified by R5. It was discovered that while the document does address R5.3, the information listed related to the authentication password controls for access to CCAs was out of date and had not been updated when a new authentication solution was implemented. The change to the CIP-007-3 R5 procedure/policy occurred in November 2010; the registered entity did not detect the issue and revise documentation until November 28, 2011. Therefore, the registered entity failed to document revised procedure within 30 days as required by CIP-007-3 R9. The registered entity had implemented procedures consistent with CIP-007-3, and its new password controls were stricter, e.g. the new systems required a minimum password length of 12 characters. The registered entity states that all password controls required by the CIP-007 R5 standard were implemented. The registered entity updated CIP-007-3 R5 documentation to reflect the revised process.

Example 2

CIP-004-1 R4

Cyber Security — Personnel & Training

R4. *Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.*

The registered entity was in violation of CIP-004-1 R4 because the registered entity failed to review the list of its personnel who have authorized cyber or authorized unescorted physical access to critical cyber assets (CCAs) quarterly. The registered entity did not review the list of personnel who were in possession of keys that allowed physical security perimeter (PSP) substation access in the cases where the card reader was out of service. Additionally, the registered entity failed to revoke access within the proper timeframe (seven days) for personnel who no longer needed to be in possession of those keys. Approximately 30-50 keys were unaccounted for from when the registered entity was required to comply with the Standard to when new locks and keys were installed. The registered entity had a documented key system in place to track key access to the outer gate and required a background check for gate access. The standard method of accessing the substation is a swipe card, and there was,

and still is, a procedure in place for tracking and revoking swipe card access. The keys at issue here are used only in the event that the swipe card system is not functioning and at no time during the violation did the swipe card system fail to force the use of the keys. These keys are numbered but otherwise unidentifiable. The registered entity has installed alarms that are generated immediately to Security if the card reader is bypassed using the key. There were no incidents at the registered entity facilities during the pendency of this violation. The registered entity installed specific lock boxes at each facility in question, and the old locks associated with the undocumented keys have been removed. Individuals no longer have a physical key to access the substation should the card reader system fail. The registered entity created a new procedure, in which just one key is kept at a separate office in a site-specific lock box with security personnel who are trained in the documented access procedure. The registered entity also violated CIP-006-1 R1. The two violations were discovered through a Self-Report.

Example 3

CIP-004-3 R2

Cyber Security — Personnel & Training

R2. *Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.*

The registered entity did not provide the proper training to two employees with granted access to CCAs. Two long-term employees were granted NERC CIP access without having completed the proper NERC training. The first employee did not complete the annual required training and upon discovery five months later, the annual training was completed promptly with satisfactory results. This employee had successfully completed 2009 and 2010 annual training, but his 2011 annual training was delayed by five months and six days. The second employee was inadvertently given access to the secured PSP and was not trained prior to having such access because the entity issued an incorrect badge to this employee. His excess access privileges to the PSP were revoked within six days. He was not aware that he had access nor did he exercise access during these six days. Also, the employees involved were long-term entity personnel with satisfactory personnel risk assessments (PRAs). The registered entity conducted a coaching session to emphasize the importance of following established procedures with staff responsible for processing card keys. The registered entity modified the desk level procedure and trained its employee groups involved in granting physical and cyber access. The registered entity had violated this Standard previously, but this instance of noncompliance did not represent a failure to mitigate the prior violation appropriately.

Example 4

CIP-005-1 R2.1 and R2.2

Cyber Security — Electronic Security Perimeter(s)

R2. *Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).*
R2.1. *These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.*
R2.2. *At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.*

The registered entity did not apply the access control model of deny by default for its identified access points and failed to implement access control rules which permit a clearly identified unique host access to only ports and services required for normal operation. The registered entity 's practice did not meet the requirement of R2.1 to provide explicit access permissions (deny by default) or R2.2 so that an access point only enables ports and services required for operations and monitoring. The firewall rules limited access to trusted networks and allowed non-interactive ports and services as the interactive ports were blocked. A total of three employees have access to the firewall rule set and configuration files. The registered entity modified its access control lists to bring firewalls within the requirements of the Standard. Some of the policy rules included a larger amount of hosts and were adjusted to be more specific. The registered entity rules were also reorganized to omit the "denies" within the ESP control areas. The registered entity also violated CIP-005-1 R2.6, CIP-005-1 R1, CIP-002-1 R3, CIP-006-1 R2, CIP-007-1 R5.3, CIP-007-1 R2, CIP-007-1 R5.2, CIP-007-1 R6.2 and R6.5, CIP-007-1 R5 and CIP-004-1 R2.1. All violations were discovered through Self-Reports.

Example 5

CIP-003-2 R1

Cyber Security — Security Management Controls

R1. *Cyber Security Policy — The Responsible Entity shall document and implement a cyber-security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:*
R1.1. *The cyber security policy addresses the requirements in Standards CIP-002-2 through CIP-009-2, including provision for emergency situations.*
R1.2*. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.*
R1.3. *Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.*

The registered entity failed to implement its cyber security policy, which requires the entity to change its passwords every 90 days. The registered entity did not implement the 90-day password policy to address any particular risk, but rather the entity based the 90-day password policy on generally accepted good practice. According to its cyber security policy, the registered entity should have changed its passwords no later than 90 days from the date the entity had to comply with CIP-003-2 R1; however, the registered entity did not change its passwords until eight months later. The registered entity's cyber security policy is more

stringent than that required by CIP-007-2 R5.3.3, which requires that a registered entity change its passwords at least annually. The registered entity did change its passwords annually, but failed to implement its internal cyber security policy, as required. The Regional Entity determined that the entity failed to implement its cyber security policy by not changing its passwords every 90 days. The registered entity mitigated the violation by changing its passwords and updating its password management process to align with CIP-007-2 R5.

Example 6

CIP-006-1 R1.8

Cyber Security — Physical Security of Critical Cyber Assets

R1. *Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:*

R1.8. *Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.*

The entity failed to secure Cyber Assets provisioning physical access control and monitoring (PACM) to its PSPs in violation of CIP-006-1 R1 R1.8. The scope of the violation included fourteen critical assets (CAs). The registered entity failed to identify two CAs as CAs provisioning access control and monitoring. The registered entity failed to afford protective measures described under CIP-005-1 R2, CIP-007-1 R2, R3, R5 and R8, and CIP-009-1 R5 to three CAs; and, the entity did not afford two protective measures (CIP-008-1 R8 and CIP-009-1 R5) to nine CAs provisioning access control and monitoring. Nine of the twelve devices in scope were identified as CAs provisioning access control and monitoring. The CAs that were not identified as access points, were equipped with protections that limited access to the entity's PACM network design. The registered entity's PSPs are dedicated to a specific network, which operates in complete isolation. The PACM network is physically and electronically isolated; access to it is controlled and monitored. The registered entity reviewed and revised its existing CIP CCA procedures to include the addition of the PACM devices; implemented each protective measure and documented successful completion of each procedure; and incorporated all PACM assets used in the access control and monitoring of the PSP into the entity's existing program for CCAs.

Example 7

CIP-006-1 R1.1

Cyber Security — Physical Security of Critical Cyber Assets

R1*. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:*

R1.1. *Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.*

The registered entity failed to locate all Cyber Assets in a defined ESP within an identified PSP and failed to incorporate a completely enclosed six-wall border for a PSP in its Physical Security Plan. The Regional Entity discovered an opening above the ceiling tiles in the breezeway connecting the control center and administration buildings. The opening allowed passage from the breezeway into the control center's designated PSP, bypassing access controls. Although the unprotected opening in the PSP boundary provided the ability to bypass access control mechanisms, access to any CCAs within the PSP requires clearance of additional access controls. The registered entity's facility is protected against unauthorized access by three levels of physical security, and also includes video surveillance, and two levels of credential check-points. Access to any CCAs within the PSP requires clearance of additional access controls. The registered entity secured the opening with wire mesh, therefore restoring the six-wall border.

Example 8

CIP-006-1 R2

Cyber Security — Physical Security of Critical Cyber Assets

R2. *Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:*

R2.1. *Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.*

R2.2. *Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.*

R2.3. *Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.*

R2.4. *Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.*

The registered entity reported that it failed to fully implement operational and procedural controls to manage physical access at all access points to six of its PSPs twenty-four hours a day, seven days a week, in violation of CIP-006-1 R2. The registered entity has installed special locks on the PSPs at issue to allow entry when card readers are inoperable. There were five keys available for the special locks (restricted keyway). The facility could not account for one key for the restricted keyways. All locks to the restricted keyways were changed as a result of the missing key. PSPs at the facility with a card reader door were also equipped with physical key locks (which were not restricted keyways) could be operated with a master key. The physical key locks on these doors were not disabled and special Locks (restricted keyways) were not installed. The assets were located inside a secured facility with armed guards, and these devices could not be remotely accessed. The duration was for 26 days for four PSPs and 45 days for two PSPs. After discovering the violation, the entity placed guards in identified rooms and manually logged access, installed and programmed card readers for identified rooms for NERC CIP access, and replaced the special keys and key cores. The entity installed a special key

lock in at least one door in each protected area and disabled the key lock access to the other doors. The entity also violated CIP-005-1 R2.6, CIP-005-1 R1, CIP-002-1 R3, CIP-005-1 R2.1 and R2.2, CIP-007-1 R5.3, CIP-007-1 R2, CIP-007-1 R5.2, CIP-007-1 R6.2 and R6.5, CIP-007-1 R5 and CIP-004-1 R2.1. All violations were discovered through Self-Reports.

Example 9

CIP-005-3 R1.1

Cyber Security — Electronic Security Perimeter(s)

R1.1 Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

The registered entity did not identify certain third-party vendor security device appliances as access points to ESPs. These appliances allow the third-party vendor to monitor activity on the entity's network and identify any unauthorized activities. These appliances are directly connected to mirrored ports on routers within the ESP. This violation involved nine of the entity's devices. The registered entity failed to identify these devices as access points to the ESP, as required by CIP-005-3 R1.1 but included these appliances on its network diagrams. The registered entity also afforded the same protections to the appliances as it provides to all access points to the ESP. Due to their being connected via mirrored ports, the appliances are only configured for monitoring traffic and for reporting anomalies out of the ESP. These appliances are not configured to carry information into the ESP. The appliances at issue are located within the PSPs. The registered entity revised its network topology diagrams to identify the appliances as access points to the ESP.

OPS and Planning Examples

Example 1

PRC-005-1 R1

Transmission and Generation Protection System Maintenance and Testing

R1. *Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:*

R1.1. *Maintenance and testing intervals and their basis.*

R1.2. *Summary of maintenance and testing procedures.*

The registered entity's relay maintenance and testing procedure lacked the following: testing intervals and the basis for intervals for CTs and PTs; testing intervals and the basis for intervals for associated communications systems; and the basis for battery testing intervals. The registered entity was testing and monitoring the protection system devices that were missing from its Protection System Testing and Maintenance Program through its SCADA system. The

registered entity was also testing its batteries according to the intervals in its plan, testing its voltage and current sensing devices simultaneously with its relays, most of which are monitored through its SCADA system, and routinely inspecting its substations, which includes checks of these devices. The registered entity was monitoring its associated communication systems through its SCADA system; testing, end to end, its channel signal strength daily, beginning at 4 a.m. and continuing until all channels are tested successfully; testing, through a low and high power test, how communications would function at half power; and performing a functional end to end testing with another entity, either at its request or at least annually. The registered entity's protection system maintenance and testing procedures were revised to include testing intervals for all required elements, as well as the basis for those intervals. Standardized inspection and testing forms were also developed to mitigate this violation.

Example 2

PRC-005-1 R2

Transmission and Generation Protection System Maintenance and Testing

R2. *Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:*

R2.1. *Evidence Protection System devices were maintained and tested within the defined intervals.*

R2.2. *Date each Protection System device was last tested/maintained.*

As a generator owner (GO), the registered entity had failed to implement its Protection System maintenance and testing programs as follows: 1) for its relay devices, the entity could not substantiate testing within a three-year interval for four (of 85) relays; 2) for its station batteries, the entity could not provide documentation of monthly battery maintenance and testing; 3) for its 20 DC control circuits, the entity could not provide documentation of the last test date; and 4) for its instrument transformers, the entity could not provide testing data after initial commission testing. The three-year interval was reasonable for the identified relays based on the entity's GOP's PRC-005-1 maintenance and testing procedures and did not materially affect the reliability of relay operation. For its batteries, the registered entity provided the manufacturer's battery maintenance document supporting its battery maintenance and testing procedures and intervals. The registered entity conducted monthly visual inspections and voltage checks for its batteries from 2010 forward and battery load tests occurring on a six-year interval. For its instrument transformers, the entity stated it conducted visual inspections during outages. The entity's affected communication systems had been tested by its TOP/GOP in 1999 and 2011. The registered entity's control room operators continuously monitor 23 of its 85 station relays, its battery bank, its 161 kV station bus, its two associated communication paths, and multiple alarm points for its five station breakers. The registered entity's facility represents only 5% of its interconnected TOP's generating resources, and its generation plant is connected to the BPS at 161 kV with a maximum output of 320 MW. This violation affected 72 (47%) out of 153 of the entity's Protection System devices. The registered entity failed to document testing for 4 relays, 2 associated communication systems,

45 instrument transformers, 1 battery bank, and 20 DC control circuits. This violation was the result of a lack of a comprehensive formal program for the scheduling and documentation. Following discovery of the violation, the entity tested all of its Protection Systems at issue, conducted staff training and automated the scheduling and the documentation of all maintenance and testing activities.

Example 3

FAC-008-1 R1

Facility Ratings Methodology

The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:
R1.1. *A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.*
R1.2. *The method by which the Rating (of major BES equipment that comprises a Facility) is determined.*
R1.2.1. *The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices,terminal equipment, and series and shunt compensation devices.*
R1.2.2. *The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.*
R1.3. *Consideration of the following:*
R1.3.1. *Ratings provided by equipment manufacturers.*
R1.3.2. *Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).*
R1.3.3. *Ambient conditions.*
R1.3.4. *Operating limitations.*
R1.3.5. *Other assumptions.*

The registered entity could not demonstrate that its Facility Rating Methodology addressed the following: The scope of equipment did not address relay protective devices and terminal equipment, as required by R1.2.1. The scope of Ratings did not include both Normal and Emergency Ratings for relay protective devices, as required by R1.2.2. The Facility Ratings Methodology did not address the following: Equipment manufacturers for relay protective devices and terminal equipment, as required by R1.3.1; design criteria, as required by R1.3.2; ambient conditions, as required by R1.3.3; operating limitations, as required by R1.3.4; and other assumptions for the following: generators, transmission conductors, transformers, relay protective devices and terminal equipment, as required by R1.3.5. The Ratings at issue were developed during the design of the Facility and the final commissioning of the plant. In a study conducted upon commissioning, it was determined that the turbines were the most limiting equipment and the entity's equipment and Ratings have not changed since commissioning. The registered entity was operating its Facility as per the manufacturer's specifications. The entity reviewed and confirmed its previous Facility Rating Methodology. The registered entity established and documented a modified nameplate listing and/or reference drawing Ratings cataloging the methodology of major BPS equipment.

Example 4

VAR-002-1.1b R3

Generator Operation for Maintaining Network Voltage Schedules

R3. *Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:*

R3.1. *A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.*

R3.2. *A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.*

The entity, as a generator operator (GOP), violated VAR-002-1.1b R3. The entity's Combustion Turbine Generator (CTG) was operating with the Automatic Voltage Regulator (AVR) in the wrong mode. The entity's generation plant is a 249 MW facility with an annual operation of less than 50 %. The entity had been operating in VAR mode instead of Voltage Control mode from August 2, 2007 until January 12, 2011, when the unit was dispatched off-line. The change to the correct AVR mode was made during the period the unit was offline from January 12, 2011 to August 24, 2011. The unit was brought back online on August 24, 2011. The entity did not notify its TOP of the change in AVR status until September 7, 2011, in violation of this Standard. The registered entity's net output of the combined cycle generation plant is based on the output of two distinct turbine-generators - the Combustion Turbine Generator (CTG) and the Steam Turbine Generator (STG). Although the entity operated the CTG's AVR in VAR mode, the STG was consistently operated in the correct Voltage Control mode. The output of the plant was always within the operating parameters defined by its TOP. The registered entity's operating personnel followed all directives given by the TOP when deviations to the voltage schedule were required. The registered entity has retrained operating personnel on startup procedures and implemented procedural changes. The registered entity also violated VAR-002-1 R1. The two violations were discovered during the self-certification process.

Example 5

FAC-009-1 R1

Establish and Communicate Facility Ratings

R1. *The Transmission Owner and Generator Owner shall each establish Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.*

The facility ratings for the registered entity did not include an equipment rating for the registered entity's generation interconnection line. Upon further review, it was determined that generation interconnection lines were to be included among the scope of equipment from which the facility's rating should be established. The line was omitted from the entity Facility Rating Methodology and ties the plant to another registered entity's transmission substation

but was not the most limiting element of the Facility. Proper coordination occurred between the entity and the other entity after review of the Interconnection Agreement. Relay settings were reviewed and did not need modification and the TOP, RC and PA were being informed of the line's rating and status at all times. No disturbances occurred on the transmission line during the violation period. The registered entity has enhanced its Facility Rating Methodology to include generation tie lines, and also updated its Facility Ratings. An updated Facilities Rating sheet was provided for the transmission line.

Example 6

FAC-008-1 R1

Facility Ratings Methodology

R1. *The Transmission Owner and Generator Owner shall each document its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities. The methodology shall include all of the following:*
R1.1. *A statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility.*
R1.2. *The method by which the Rating (of major BES equipment that comprises a Facility) is determined.*
R1.2.1. *The scope of equipment addressed shall include, but not be limited to, generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.*
R1.2.2. *The scope of Ratings addressed shall include, as a minimum, both Normal and Emergency Ratings.*
R1.3. *Consideration of the following:*
R1.3.1. *Ratings provided by equipment manufacturers.*
R1.3.2. *Design criteria (e.g., including applicable references to industry Rating practices such as manufacturer's warranty, IEEE, ANSI or other standards).*
R1.3.3. *Ambient conditions.*
R1.3.4. *Operating limitations.*
R1.3.5. *Other assumptions.*

The registered entity's generation Facility Ratings Methodology (FRM) did not address the entire scope of equipment required by FAC-008-1 R1. A Regional Entity audit team reported an additional violation of FAC-008-1 R1 after finding that the entity was unable to provide evidence of a documented generation FRM from June 18, 2007 through August 27, 2007. The registered entity's generation FRM in place after August 27, 2007 failed to address relay protective devices, terminal equipment, and series and shunt compensation devices. The registered entity, as a GO, was in violation of FAC-008-1 R1 because it did not have an FRM prior to August 27, 2007, and once it adopted an FRM, did not address all necessary equipment. The registered entity's FRM was designed to reflect the most limiting element, the generator, and once revised, the Facility Rating did not change. The Facilities at issue were rated based on manufacturer's ratings and the units had been operated in accordance with those Ratings. On May 28, 2010, the entity registered as a Transmission Owner (TO). The registered entity stated that it believed its generation FRM was sufficient for its GO and TO functions. The Regional Entity staff reviewed the entity's generation FRM and found it did not address Facility Ratings

for the TO function. The Regional Entity determined that the entity, as a TO, was in violation of FAC-008-1 R1 for not having an FRM that covered its transmission equipment. The registered entity revised and consolidated its procedures to address both generation and transmission facilities and to include all equipment listed in FAC-008-1 R1.2.1, and updated its FRM to include all relevant generation and transmission equipment.

Example 7

VAR-002-1.1a R3

Generator Operation for Maintaining Network Voltage Schedules

R3. *Each Generator Operator shall notify its associated Transmission Operator as soon as practical, but within 30 minutes of any of the following:*

R3.1. *A status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.*

R3.2. *A status or capability change on any other Reactive Power resources under the Generator Operator's control and the expected duration of the change in status or capability.*

The registered entity did not notify its TOP of the status change in the AVR operation. Specifically, one of the registered entity's units was inadvertently changed by the operator from automatic voltage control mode to manual mode and the entity did not notify its associated TOP within 30 minutes. The registered entity's unit operated in manual mode for four hours prior to shut down. The incident involved only one unit at the facility, which consists of three units with a total capacity of over 500 MW. The unit maintained its voltage schedule during the violation period. The registered entity reported the change in status to the TOP approximately a week later. After reviewing its records, the registered entity did not identify any other instance of its generators operating with its AVR out of service without appropriate communication to its TOP. The registered entity moved the AVR switch to a different computer screen in order to prevent an inadvertent change from AVR to Manual mode in the future, added a computer screen indicator flag to remind operators to notify the TOP of a change in status, and trained its plant operations staff regarding the appropriate actions to take in the event of a status change.

Example 8

PER-003-0 R1

Operating Personnel Credentials

R1. *Each Transmission Operator, Balancing Authority, and Reliability Coordinator shall staff all operating positions that meet both of the following criteria with personnel that are NERC certified for the applicable functions:*

R1.1. *Positions that have the primary responsibility, either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System.*

R1.2. *Positions directly responsible for complying with NERC standards.*

In conjunction with its registration efforts, the registered entity submitted a TOP Implementation Plan to the Regional Entity that was accepted. The purpose of the Implementation Plan was to address certain deficiencies the entity identified in preparation for

its TOP Certification Review. Prior to the registered entity's TOP registration, the registered entity was not required to staff NERC-certified operators. The Implementation Plan required that all appropriate operators on staff would be NERC-certified by March 2011. On April 26, 2011, the Regional Entity conducted an Audit and determined that the registered entity failed to meet the deadline for having the operators certified, in violation of PER-003-0 R1.1 and R1.2. The registered entity operators on staff had received extensive training and demonstrated competency in their jobs' duties. The training for the entity operators took place in March 2010 with the balance of operators participating in the training in May 2011; there was additional training in November 2010, February 2011 and November 2011. Some examples of the training are: (1) All system operators enrolled in a certification preparation course and training program;(2) the entity made available to all system operators and control room staff various tutorials and practices; (3) All the registered entity system operators and control room staff have attended a NERC Reliability Standards course from a third party training program. After discussion with the Regional Entity, the registered entity delegated specific TOP activities to a registered TOP which provided NERC certified operators to operate the registered entity's transmission system.

Example 9

EOP-005-1 R1

System Restoration Plans

R1. *Each Transmission Operator shall have a restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system, including necessary operating instructions and procedures to cover emergency conditions, and the loss of vital telecommunications channels. Each Transmission Operator shall include the applicable elements listed in Attachment 1-EOP-005 in developing a restoration plan.*

The registered entity could not show that several system operators received System Restoration training as required by Attachment 1 to EOP-005-1 (Elements for Consideration in Development of Restoration Plans) Element # 7, which states that documentation must be retained in the personnel training records that operating personnel have been trained annually in the implementation of the plan and have participated in restoration exercises. After further review, the registered entity determined that it did not have evidence that several system operators received System Restoration training, as required by this Standard. The registered entity had evidence that the system operators had performed multiple system restoration training simulations in the past and after the violation was discovered. Each of the system operators had participated in some training and was familiar with system restoration.

Example 10

COM-002-2 R2

Communication and Coordination

R2. *Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.*

The registered entity was in violation of COM-002-2 R2 because the registered entity's control room operator failed to issue directives in a clear, concise, and definitive manner. When issuing a directive to perform switching at a substation, the registered entity control room operator did not use the proper communication technique. Further, the control room operator did not ensure that the recipient of the communication repeated the information back correctly, as required by the Standard. The operator at the substation willingly accepted the switching order and performed the switching without incident. The communication at issue was given during a period of restoration of equipment, and therefore took place under normal system conditions. The directive which was given in an improper manner was carried out by the recipient in the correct manner. Following the violation, the registered entity began random auditing of three-part communications of Security and System Operator communications and performed enhanced internal refresher training to relevant personnel.

Example 11

TOP-004-2 R1

Transmission Operations

R1. *Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).*

The registered entity, as a TOP, violated TOP-004-2 R1. During a one-day event on January 13, 2011, a failed static wire resulted in the outage of two 138 kV transmission lines. These outages led to what appeared to be MVA limit conditions on a 230/138 kV autotransformer. Although the SOL was exceeded because the autotransformer had been rated conservatively, there was no Interconnection Reliability Operating Limit (IROL) exceedance. The system operator initiated a load shed of the entity's local load (approximately 135 MW) for approximately one hour to resolve what appeared to be a transformer overload. There was no instability, uncontrolled separation, or cascading outages nor would they have resulted from the loss of the transformer. Tests performed after the event indicated that the autotransformer in question had been rated conservatively and was not overloaded, had not been damaged and was not at risk of failure. Even if the transformer had tripped, the result would have been limited to loss of local entity internal load. The manual load shed performed to correct the exceedance affected only local load. Also, although there appeared to be an overload on the autotransformer, due primarily to cold weather, the autotransformer was never actually overloaded because it had been rated conservatively. This was confirmed by subsequent review of industry standards, dissolved gas analysis and electrical testing of the autotransformer which showed the transformer was actually under rated. The registered entity enhanced its Facility Rating Methodology to include flexibility to account for cold weather conditions and the specific characteristics of autotransformers and other power system equipment to address real-time conditions. A new Methodology was developed by entity operations to include normal and emergency winter Ratings. System operations procedures were updated to include a specific list of actions to take in anticipation of and during cold weather conditions.

Example 12

PRC-008-0 R2

Implementation and Documentation of Underfrequency Load Shedding Equipment Maintenance Program

R2. *The Transmission Owner and Distribution Provider with a UFLS program (as required by its Regional Reliability Organization) shall implement its UFLS equipment maintenance and testing program and shall provide UFLS maintenance and testing program results to its Regional Reliability Organization and NERC on request (within 30 calendar days).*

The registered entity did not have maintenance and testing records of station batteries associated with its Underfrequency Load Shedding (UFLS) program. The registered entity provided the past maintenance and testing dates and the most recent UFLS relay maintenance and testing records. The registered entity was not able to provide evidence of weekly pilot cell voltage and specific gravity readings or the annual cell voltage, cell impedance or strap resistance testing of its station batteries used in its UFLS program. The registered entity has 21 UFLS devices subject to PRC-008-0 R2. Of the 21 devices, the entity failed to provide evidence of maintenance and testing for 2 devices, or approximately 9.5%. Specifically, the registered entity failed to provide evidence of maintenance and testing for 2 station batteries. The registered entity only has two interconnection points and could shed 23 MW of UFLS load. The registered entity reviewed its maintenance and testing policy and has adjusted the testing of the station batteries. The weekly test of the pilot cell voltage and specific gravity has been changed to a monthly test, and the registered entity is recording the temperature of the pilot cell.

Defined Acronyms

Term	Acronym	Definition
Current Transformer(s)	CT(s)	An instrument transformer used to transform current for use in monitoring and control systems
Critical Asset(s)	CA(s)	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
Critical Cyber Asset(s)	CCA(s)	Cyber Assets essential to the reliable operation of Critical Assets.
Electronic Security Perimeter	ESP	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Interconnection Reliability Operating Limit	IROL	The value (such as MW, MVar, Amperes, Frequency or Volts) derived from, or a subset of the System Operating Limits, which if exceeded, could expose a widespread area of the Bulk Electric System to instability, uncontrolled separation(s) or cascading outages.
Personnel Risk Assessment	PRA	An assessment conducted for personnel having access to critical cyber assets, that includes, at least, identity verification and seven-year criminal check
Physical Security Perimeter	PSP	The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.
Potential Transformer(s)	PT(s)	An instrument transformer used to transform voltage for use in monitoring and control systems
Supervisory Control and Data Acquisition System	SCADA	A system of remote control and telemetry used to monitor and control the transmission system.
System Operating Limit	SOL	The value (such as MW, MVar, Amperes, Frequency or Volts) that satisfies the most limiting of the prescribed operating criteria for a specified system configuration to ensure operation within acceptable reliability criteria. System Operating Limits are based upon certain operating criteria. These include, but are not limited to: • Facility Ratings (Applicable pre- and post-Contingency equipment or facility ratings) • Transient Stability Ratings (Applicable pre- and post-Contingency Stability Limits) • Voltage Stability Ratings (Applicable pre- and post-Contingency Voltage Stability) • System Voltage Limits (Applicable pre- and post-Contingency Voltage Limits)

*All functions are in abbreviated form.

Exhibit C

Instructors Training

September 19 – 20, 2012 - Atlanta, GA

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Instructors Training

Atlanta

September 19-20, 2012

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Critical Infrastructure Protection (CIP) Examples - FFTs

Example 1

CIP-007-3 R9 Violation Risk Factor (VRF): Lower; Violation Severity Level (VSL): High)

The registered entity failed to document changes made to CIP-007-3 R5 procedure/policy within 30 days, pursuant to CIP-007-3 R9. The department responsible for the support of the network devices in the energy management system (EMS) environment created a process document to capture the procedures and policies for "account management" as specified by R5. It was discovered that while the document does address R5.3, the information listed related to the authentication password controls for access to critical cyber assets (CCAs) was out of date and had not been updated when a new authentication solution was implemented. The change to the CIP-007-3 R5 procedure/policy occurred in November 2010; the registered entity did not detect the issue and revise documentation until November 28, 2011. Therefore, the registered entity failed to document revised procedure within 30 days as required by CIP-007-3 R9. The registered entity had implemented procedures consistent with CIP-007-3, and its new password controls were stricter, e.g. the new systems required a minimum password length of 12 characters. The registered entity states that all password controls required by the CIP-007 R5 standard were implemented. The registered entity updated CIP-007-3 R5 documentation to reflect the revised process.

Example 2

CIP-004-3 R2 (VRF: Lower; VSL: Severe)

The registered entity did not provide the proper training to two employees with granted access to CCAs. Two long-term employees were granted NERC CIP access without having completed the proper NERC training. The first employee did not complete the annual required training and upon discovery five months later, the annual training was completed promptly with satisfactory results. This employee had successfully completed 2009 and 2010 annual training, but his 2011 annual training was delayed by five months and six days. The second employee was inadvertently given access to the secured physical security perimeter (PSP) and was not trained prior to having such access because the registered entity issued an incorrect badge to this employee. His excess access privileges to the PSP were revoked within six days. He was not aware that he had access nor did he exercise access during these six days. Also, the employees involved were long-term registered entity personnel with satisfactory personnel risk assessments (PRAs). The registered entity conducted a coaching session to emphasize the importance of following established procedures with staff responsible for processing card keys. The registered entity modified the desk level procedure and trained its employee groups involved in granting physical and cyber access. The registered entity had violated this Standard previously but this instance of noncompliance did not represent a failure to mitigate the prior violation appropriately.

Example 3

CIP-003-2 R1 (VRF: Medium; VSL: Severe)

The registered entity failed to implement its cyber security policy, which requires the registered entity to change its passwords every 90 days. The registered entity did not implement the 90-day password policy to address any particular risk, but rather the registered entity based the 90-day password policy on generally accepted good practice. According to its cyber security policy, the registered entity should have changed its passwords no later than 90 days from the date the registered entity had to comply with CIP-003-2 R1; however, the registered entity did not change its passwords until eight months later. The registered entity's cyber security policy is more stringent than that required by CIP-007-2 R5.3.3, which requires that a registered registered entity change its passwords at least annually. The registered entity did change its passwords annually, but failed to implement its internal cyber security policy, as required. The Regional Entity determined that the registered entity failed to implement its cyber security policy by not changing its passwords every 90 days. The registered entity mitigated the violation by changing its passwords and updating its password management process to align with CIP-007 R5.

Example 4

CIP-006-1 R1.1 (VRF: Medium; VSL: Severe)

The registered entity failed to locate all Cyber Assets in a defined electronic security perimeter (ESP) within an identified PSP and failed to incorporate a completely enclosed six-wall border for a PSP in its Physical Security Plan. The Regional Entity discovered an opening above the ceiling tiles in the breezeway connecting the control center and administration buildings. The opening allowed passage from the breezeway into the control center's designated PSP, bypassing access controls. Although the unprotected opening in the PSP boundary provided the ability to bypass access control mechanisms, access to any CCAs within the PSP requires clearance of additional access controls. The registered entity's facility is protected against unauthorized access by three levels of physical security, and also includes video surveillance, and two levels of credential check-points. Access to any CCAs within the PSP requires clearance of additional access controls. The registered entity secured the opening with wire mesh, therefore restoring the six-wall border.

Example 5

CIP-005-3 R1.1 (VRF: Medium; VSL: Severe)

The registered entity did not identify certain third-party vendor security device appliances as access points to ESPs. These appliances allow the third-party vendor to monitor activity on the registered entity's network and identify any unauthorized activities. These appliances are directly connected to mirrored ports on routers within the ESP. This violation involved nine of the registered entity's devices. The registered entity failed to identify these devices as access points to the ESP, as required by CIP-005-3 R1.1 but included these appliances on its network diagrams. The registered entity also afforded the same protections to the appliances as it provides to all access points to the ESP. Due to their being connected via mirrored ports, the appliances are only configured for monitoring traffic and for reporting anomalies out of the

ESP. These appliances are not configured to carry information into the ESP. The appliances at issue are located within the PSPs. The registered entity revised its network topology diagrams to identify the appliances as access points to the ESP.

CIP Examples – SNOPs

Example 1

CIP-004-1 R4 (VRF: Medium; VSL: Severe)

The registered entity was in violation of CIP-004-1 R4 because the registered entity failed to review the list of its personnel who have authorized cyber or authorized unescorted physical access to CCAs quarterly. The registered entity did not review the list of personnel who were in possession of keys that allowed PSP substation access in the cases where the card reader was out of service. Additionally, the registered entity failed to revoke access within the proper timeframe (seven days) for personnel who no longer needed to be in possession of those keys. Approximately 30-50 keys were unaccounted for from when the registered entity was required to comply with the Standard to when new locks and keys were installed. The registered entity had a documented key system in place to track key access to the outer gate and required a background check for gate access. The standard method of accessing the substation is a swipe card, and there was, and still is, a procedure in place for tracking and revoking swipe card access. The keys at issue here are used only in the event that the swipe card system is not functioning and at no time during the violation did the swipe card system fail to force the use of the keys. These keys are numbered but otherwise unidentifiable. The registered entity has installed alarms that are generated immediately to Security if the card reader is bypassed using the key. There were no incidents at the registered entity facilities during the pendency of this violation. The registered entity installed specific lock boxes at each facility in question, and the old locks associated with the undocumented keys have been removed. Individuals no longer have a physical key to access the substation should the card reader system fail. The registered entity created a new procedure, in which just one key is kept at a separate office in a site-specific lock box with security personnel who are trained in the documented access procedure. The registered entity also violated CIP-006-1 R1. The two violations were discovered through a Self-Report.

Example 2

CIP-005-1 R2.1 and R2.2 (VRF: Medium; VSL: Moderate)

The registered entity did not apply the access control model of deny by default for its identified access points and failed to implement access control rules which permit a clearly identified unique host access to only ports and services required for normal operation. The registered entity's practice did not meet the requirement of R2.1 to provide explicit access permissions (deny by default) or R2.2 so that an access point only enables ports and services required for operations and monitoring. The firewall rules limited access to trusted networks and allowed non-interactive ports and services as the interactive ports were blocked. A total of three employees have access to the firewall rule set and configuration files. The registered entity

modified its access control lists to bring firewalls within the requirements of the Standard. Some of the policy rules included a larger amount of hosts and were adjusted to be more specific. The registered entity rules were also reorganized to omit the "denies" within the ESP control areas. The registered entity also violated CIP-005-1 R2.6, CIP-005-1 R1, CIP-002-1 R3, CIP-006-1 R2, CIP-007-1 R5.3, CIP-007-1 R2, CIP-007-1 R5.2, CIP-007-1 R6.2 and R6.5, CIP-007-1 R5 and CIP-004-1 R2.1. All violations were discovered through Self-Reports.

Example 3

CIP-006-1 R1.8 (VRF: Lower; VSL: Severe)

The registered entity failed to secure Cyber Assets provisioning physical access control and monitoring (PACM) to its PSPs in violation of CIP-006-1 R1 R1.8. The scope of the violation included fourteen Critical Assets (CAs). The registered entity failed to identify two CAs as CAs provisioning access control and monitoring. The registered entity failed to afford protective measures described under CIP-005-1 R2, CIP-007-1 R2, R3, R5 and R8, and CIP-009-1 R5 to three CAs; and, the registered entity did not afford two protective measures (CIP-008-1 R8 and CIP-009-1 R5) to nine CAs provisioning access control and monitoring. Nine of the twelve devices in scope were identified as CAs provisioning access control and monitoring. The CAs that were not identified as access points were equipped with protections that limited access to the registered entity's PACM network design. The registered entity's PSPs are dedicated to a specific network, which operates in complete isolation. The PACM network is physically and electronically isolated; access to it is controlled and monitored. The registered entity reviewed and revised its existing CIP CCA procedures to include the addition of the PACM devices; implemented each protective measure and documented successful completion of each procedure; and incorporated all PACM assets used in the access control and monitoring of the PSP into the registered entity's existing program for CCAs.

Example 4

CIP-006-1 R2 (VRF: Medium; VSL: High)

The registered entity reported that it failed to fully implement operational and procedural controls to manage physical access at all access points to six of its PSPs twenty-four hours a day, seven days a week, in violation of CIP-006-1 R2. The registered entity has installed special locks on the PSPs at issue to allow entry when card readers are inoperable. There were five keys available for the special locks (restricted keyway). The facility could not account for one key for the restricted keyways. All locks to the restricted keyways were changed as a result of the missing key. PSPs at the facility with a card reader door were also equipped with physical key locks (which were not restricted keyways) could be operated with a master key. The physical key locks on these doors were not disabled and special Locks (restricted keyways) were not installed. The assets were located inside a secured facility with armed guards, and these devices could not be remotely accessed. The duration was for 26 days for four PSPs and 45 days for two PSPs. After discovering the violation, the registered entity placed guards in identified rooms and manually logged access, installed and programmed card readers for identified rooms for NERC CIP access, and replaced the special keys and key cores. The registered entity installed a special key lock in at least one door in each protected area and disabled the key lock access to the other doors. The registered entity also violated CIP-005-1 R2.6, CIP-005-1 R1, CIP-002-1 R3,

CIP-005-1 R2.1 and R2.2, CIP-007-1 R5.3, CIP-007-1 R2, CIP-007-1 R5.2, CIP-007-1 R6.2 and R6.5, CIP-007-1 R5 and CIP-004-1 R2.1. All violations were discovered through Self-Reports.

OPS and Planning Examples - FFTs

Example 1

PRC-005-1 R1 (VRF: High; VSL: Severe)

The registered entity's relay maintenance and testing procedure lacked the following: testing intervals and the basis for intervals for CTs and PTs; testing intervals and the basis for intervals for associated communications systems; and the basis for battery testing intervals. The registered entity was testing and monitoring the protection system devices that were missing from its Protection System Testing and Maintenance Program through its supervisory control and data acquisition (SCADA) system. The registered entity was also testing its batteries according to the intervals in its plan, testing its voltage and current sensing devices simultaneously with its relays, most of which are monitored through its SCADA system, and routinely inspecting its substations, which includes checks of these devices. The registered entity was monitoring its associated communication systems through its SCADA system; testing, end to end, its channel signal strength daily, beginning at 4 a.m. and continuing until all channels are tested successfully; testing, through a low and high power test, how communications would function at half power; and performing a functional end to end testing with another registered entity, either at its request or at least annually. The registered entity's protection system maintenance and testing procedures were revised to include testing intervals for all required elements, as well as the basis for those intervals. Standardized inspection and testing forms were also developed to mitigate this violation.

Example 2

FAC-008-1 R1 (VRF: Lower; VSL: Severe)

The registered entity could not demonstrate that its Facility Rating Methodology addressed certain issues. The scope of equipment did not address relay protective devices and terminal equipment, as required by R1.2.1. The scope of Ratings did not include both Normal and Emergency Ratings for relay protective devices, as required by R1.2.2. The Facility Ratings Methodology did not address the following: Equipment manufacturers for relay protective devices and terminal equipment, as required by R1.3.1; design criteria, as required by R1.3.2; ambient conditions, as required by R1.3.3; operating limitations, as required by R1.3.4; and other assumptions for the following: generators, transmission conductors, transformers, relay protective devices and terminal equipment, as required by R1.3.5. The Ratings at issue were developed during the design of the Facility and the final commissioning of the plant. In a study conducted upon commissioning, it was determined that the turbines were the most limiting equipment and the registered entity's equipment and Ratings have not changed since commissioning. The registered entity was operating its Facility as per the manufacturer's specifications. The registered entity reviewed and confirmed its previous Facility Rating Methodology. The registered entity established and documented a modified nameplate listing and/or reference drawing Ratings cataloging the methodology of major BPS equipment.

Example 3

FAC-009-1 R1 (VRF: Medium; VSL: Moderate)

The facility ratings for the registered entity did not include an equipment rating for the registered entity's generation interconnection line. Upon further review, it was determined that generation interconnection lines were to be included among the scope of equipment from which the facility's rating should be established. The line was omitted from the registered entity Facility Rating Methodology and ties the plant to another registered entity's transmission substation but was not the most limiting element of the Facility. Proper coordination occurred between the registered entity and the other registered entity after review of the Interconnection Agreement. Relay settings were reviewed and did not need modification and the transmission operator, reliability coordinator and planning authority (TOP, RC and PA), were being informed of the line's rating and status at all times. No disturbances occurred on the transmission line during the violation period. The registered entity has enhanced its Facility Rating Methodology to include generation tie lines, and also updated its Facility Ratings. An updated Facilities Rating sheet was provided for the transmission line.

Example 4

VAR-002-1.1a R3 (VRF: Medium; VSL: Lower)

The registered entity did not notify its TOP of the status change in the automatic voltage regulator (AVR) operation. Specifically, one of the registered entity's units was inadvertently changed by the operator from automatic voltage control mode to manual mode and the registered entity did not notify its associated TOP within 30 minutes. The registered entity's unit operated in manual mode for four hours prior to shut down. The incident involved only one unit at the facility, which consists of three units with a total capacity of over 500 MW. The unit maintained its voltage schedule during the violation period. The registered entity reported the change in status to the TOP approximately a week later. After reviewing its records, the registered entity did not identify any other instance of its generators operating with its AVR in other than automatic mode without appropriate communication to its TOP. The registered entity moved the AVR switch to a different computer screen in order to prevent an inadvertent change from AVR to Manual mode in the future, added a computer screen indicator flag to remind operators to notify the TOP of a change in status, and trained its plant operations staff regarding the appropriate actions to take in the event of a status change.

Example 5

EOP-005-1 R1 (VRF: Medium; VSL: Lower)

The registered entity could not show that several system operators received System Restoration training as required by Attachment 1 to EOP-005-1 (Elements for Consideration in Development of Restoration Plans) Element # 7, which states that documentation must be retained in the personnel training records that operating personnel have been trained annually in the implementation of the plan and have participated in restoration exercises. After further review, the registered entity determined that it did not have evidence that several system operators received System Restoration training, as required by this Standard. The registered entity had evidence that the system operators had performed multiple system restoration training simulations in the past and after the violation was discovered. Each of the system operators had participated in some training and was familiar with system restoration.

Example 6

PRC-008-0 R2 (VRF: Medium; VSL: Lower)

The registered entity did not have maintenance and testing records of station batteries associated with its Underfrequency Load Shedding (UFLS) program. The registered entity provided the past maintenance and testing dates and the most recent UFLS relay maintenance and testing records. The registered entity was not able to provide evidence of weekly pilot cell voltage and specific gravity readings or the annual cell voltage, cell impedance or strap resistance testing of its station batteries used in its UFLS program. The registered entity has 21 UFLS devices subject to PRC-008-0 R2. Of the 21 devices, the registered entity failed to provide evidence of maintenance and testing for 2 devices, or approximately 9.5%. Specifically, the registered entity failed to provide evidence of maintenance and testing for 2 station batteries. The registered entity only has two interconnection points and could shed 23 MW of UFLS load. The registered entity reviewed its maintenance and testing policy and has adjusted the testing of the station batteries. The weekly test of the pilot cell voltage and specific gravity has been changed to a monthly test, and the registered entity is recording the temperature of the pilot cell.

OPS and Planning Examples - SNOPs

Example 1

PRC-005-1 R2 (VRF: High; VSL: Moderate)

As a generator owner (GO), the registered entity had failed to implement its Protection System maintenance and testing programs as follows: 1) for its relay devices, the registered entity could not substantiate testing within a three-year interval for four (of 85) relays; 2) for its station batteries, the registered entity could not provide documentation of monthly battery maintenance and testing; 3) for its 20 DC control circuits, the registered entity could not provide documentation of the last test date; and 4) for its instrument transformers, the registered entity could not provide testing data after initial commission testing. The three-year interval was reasonable for the identified relays based on the registered entity's GOP's PRC-005-1 maintenance and testing procedures and did not materially affect the reliability of relay operation. For its batteries, the registered entity provided the manufacturer's battery maintenance document supporting its battery maintenance and testing procedures and intervals. The registered entity conducted monthly visual inspections and voltage checks for its batteries from 2010 forward and battery load tests occurring on a six-year interval. For its instrument transformers, the registered entity stated it conducted visual inspections during outages. The registered entity's affected communication systems had been tested by its TOP/GOP in 1999 and 2011. The registered entity's control room operators continuously monitor 23 of its 85 station relays, its battery bank, its 161 kV station bus, its two associated communication paths, and multiple alarm points for its five station breakers. The registered entity's facility represents only 5% of its interconnected TOP's generating resources, and its generation plant is connected to the BPS at 161 kV with a maximum output of 320 MW. This violation affected 72 (47%) out of 153 of the registered entity's Protection System devices. The

registered entity failed to document testing for 4 relays, 2 associated communication systems, 45 instrument transformers, 1 battery bank, and 20 DC control circuits. This violation was the result of a lack of a comprehensive formal program for the scheduling and documentation. Following discovery of the violation, the registered entity tested all of its Protection Systems at issue, conducted staff training and automated the scheduling and the documentation of all maintenance and testing activities.

Example 2

VAR-002-1.1b R3 (VRF: Medium; VSL: High)

The registered entity, as a GOP, violated VAR-002-1.1b R3. The registered entity's Combustion Turbine Generator (CTG) was operating with the Automatic Voltage Regulator (AVR) in the wrong mode. The registered entity's generation plant is a 249 MW facility with an annual operation of less than 50 %. The registered entity had been operating in VAR mode instead of Voltage Control mode from August 2, 2007 until January 12, 2011, when the unit was dispatched off-line. The change to the correct AVR mode was made during the period the unit was offline from January 12, 2011 to August 24, 2011. The unit was brought back online on August 24, 2011. The registered entity did not notify its TOP of the change in AVR status until September 7, 2011, in violation of this Standard. The registered entity's net output of the combined cycle generation plant is based on the output of two distinct turbine-generators - the Combustion Turbine Generator (CTG) and the Steam Turbine Generator (STG). Although the registered entity operated the CTG's AVR in VAR mode, the STG was consistently operated in the correct Voltage Control mode. The output of the plant was always within the operating parameters defined by its TOP. The registered entity's operating personnel followed all directives given by the TOP when deviations to the voltage schedule were required. The registered entity has retrained operating personnel on startup procedures and implemented procedural changes. The registered entity also violated VAR-002-1 R1. The two violations were discovered during the self-certification process.

Example 3

FAC-008-1 R1 (VRF: Medium; VSL: Severe)

The registered entity’s generation Facility Ratings Methodology (FRM) did not address the entire scope of equipment required by FAC-008-1 R1. A Regional Entity audit team reported an additional violation of FAC-008-1 R1 after finding that the registered entity was unable to provide evidence of a documented generation FRM from June 18, 2007 through August 27, 2007. The registered entity's generation FRM in place after August 27, 2007 failed to address relay protective devices, terminal equipment, and series and shunt compensation devices. The registered entity, as a GO, was in violation of FAC-008-1 R1 because it did not have an FRM prior to August 27, 2007, and once it adopted an FRM, did not address all necessary equipment. The registered entity's FRM was designed to reflect the most limiting element, the generator, and once revised, the Facility Rating did not change. The Facilities at issue were rated based on manufacturer's ratings and the units had been operated in accordance with those Ratings. On May 28, 2010, the registered entity registered as a Transmission Owner (TO). The registered entity stated that it believed its generation FRM was sufficient for its GO and TO functions. The Regional Entity staff reviewed the registered entity's generation FRM and found it did not address Facility Ratings for the TO function. The Regional Entity determined that the registered

entity, as a TO, was in violation of FAC-008-1 R1 for not having an FRM that covered its transmission equipment. The registered entity revised and consolidated its procedures to address both generation and transmission facilities and to include all equipment listed in FAC-008-1 R1.2.1, and updated its FRM to include all relevant generation and transmission equipment.

Example 4

PER-003-0 R1 (VRF: High; VSL: Severe)

In conjunction with its registration efforts, the registered entity submitted a TOP Implementation Plan to the Regional Entity that was accepted. The purpose of the Implementation Plan was to address certain deficiencies the registered entity identified in preparation for its TOP Certification Review. Prior to the registered entity's TOP registration, the registered entity was not required to staff NERC-certified operators. The Implementation Plan required that all appropriate operators on staff would be NERC-certified by March 2011. On April 26, 2011, the Regional Entity conducted an Audit and determined that the registered entity failed to meet the deadline for having the operators certified, in violation of PER-003-0 R1.1 and R1.2. The registered entity operators on staff had received extensive training and demonstrated competency in their jobs' duties. The training for the registered entity operators took place in March 2010 with the balance of operators participating in the training in May 2011; there was additional training in November 2010, February 2011 and November 2011. Some examples of the training are: (1) all system operators enrolled in a certification preparation course and training program; (2) the registered entity made available to all system operators and control room staff various tutorials and practices; (3) all the registered entity system operators and control room staff have attended a NERC Reliability Standards course from a third party training program. After discussion with the Regional Entity, the registered entity delegated specific TOP activities to a registered TOP which provided NERC certified operators to operate the registered entity’s transmission system.

Example 5

COM-002-2 R2 (VRF: Medium; VSL: Severe)

The registered entity was in violation of COM-002-2 R2 because the registered entity’s control room operator failed to issue directives in a clear, concise, and definitive manner. When issuing a directive to perform switching at a substation, the registered entity control room operator did not use the proper communication technique. Further, the control room operator did not ensure that the recipient of the communication repeated the information back correctly, as required by the Standard. The operator at the substation accepted the switching order and performed the switching without incident. The communication at issue was given during a period of restoration of equipment, and therefore took place under normal system conditions. The directive which was given in an improper manner was carried out by the recipient in the correct manner. Following the violation, the registered entity began random auditing of three-part communications of Security and System Operator communications and performed enhanced internal refresher training to relevant personnel.

Example 6

TOP-004-2 R1 (VRF: High; VSL: High)

The registered entity, as a TOP, violated TOP-004-2 R1. During a one-day event on January 13, 2011, a failed static wire resulted in the outage of two 138 kV transmission lines. These outages led to what appeared to be MVA limit conditions on a 230/138 kV autotransformer. Although the system operating limit (SOL) was exceeded because the autotransformer had been rated conservatively, there was no Interconnection Reliability Operating Limit (IROL) exceedance. The system operator initiated a load shed of the registered entity's local load (approximately 135 MW) for approximately one hour to resolve what appeared to be a transformer overload. There was no instability, uncontrolled separation, or cascading outages nor would they have resulted from the loss of the transformer. Tests performed after the event indicated that the autotransformer in question had been rated conservatively and was not overloaded, had not been damaged and was not at risk of failure. Even if the transformer had tripped, the result would have been limited to loss of local registered entity internal load. The manual load shed performed to correct the SOL exceedance affected only local load. Also, although there appeared to be an overload on the autotransformer, due primarily to cold weather, the autotransformer was never actually overloaded because it had been rated conservatively. This was confirmed by subsequent review of industry standards, dissolved gas analysis and electrical testing of the autotransformer which showed the transformer was actually under rated. The registered entity enhanced its Facility Rating Methodology to include flexibility to account for cold weather conditions and the specific characteristics of autotransformers and other power system equipment to address real-time conditions. A new Methodology was developed by registered entity operations to include normal and emergency winter Ratings. System operations procedures were updated to include a specific list of actions to take in anticipation of and during cold weather conditions.

Answer Key CIP FFT Examples

Example 1

CIP-007-3 R9

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue- the new password controls implemented were stricter than the previous ones and required a minimum password length of 12 characters. Also, the registered entity implemented all password controls required by this Standard and only failed to properly document these controls.

Although the issue lasted for about one year, the risk to the BPS during this period was minimal because the password requirements during this period were met.

The registered entity had a process to review and updated the documentation specified in Standard CIP-007-3 at least annually, as evidenced by the fact that the issue was discovered a year later on November 28, 2010.

Mitigation was completed relatively fast, as it only required the registered entity to update its documentation.

Example 2

CIP-004-3 R2

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue- the first employee had two years of previous training and was a long-term employee with a properly conducted PRA. The issue lasted for five months, but these mitigating factors reduced the risk to the BPS to minimal.

For the second employee, the risk was mitigated to minimal by the fact that he had a PRA, there was no attempt to access the PSPs and that the issue lasted for a short period of time.

There were no serious shortcomings in the registered entity's reliability related process, as evidenced by the fact that the two instances were discovered and mitigated immediately.

Example 3

CIP-003-2 R1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue- the registered entity's policy was more stringent than the one required by the Standards, thereby reducing the risk to the BPS to minimal. Also, the registered entity changed the password according to generally accepted practices. The facts do not indicate other shortcomings in the registered entity's cyber security program.

Although the violation lasted for about eight months, during this time, the risk to the BPS was minimal because of the factors listed above.

Example 4

CIP-006-1 R1.1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue-although the unprotected opening in the PSP boundary provided the ability to bypass access control mechanisms, access

to any CCAs requires clearance of additional access controls. Also, the opening was above the ceiling tiles in the breezeway, where any unauthorized access would have been detected easily.

The issue was mitigated immediately during the spot check.

Example 5

CIP-005-3 R1.1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

The issue was in documenting properly the security device appliances as access points to ESPs but at all relevant times provided the requisite protections to the appliances.

There were mitigating factors during the pendency of the issue- the registered entity included these appliances on its network diagrams and afforded the same protections to the appliances as it provides to all access points to the ESP. Also, the appliances were not configured to carry information into the ESP, which further reduced the risk to the BPS.

The issue was mitigated immediately during the compliance audit.

Answer Key CIP SNOP Examples

Example 1

CIP-004-1 R4

Reasons for SNOP treatment:

Risk to the reliability of the BPS: Minimal

The violation involves two instances of noncompliance. First, the registered entity did not review the list of personnel in possession of keys that allowed PSP access. Second, the registered entity failed to revoke access for personnel that no longer needed to be in possession of those keys. As a result, the registered entity left as many as 30-50 keys unaccounted for during the violation period.

There were mitigating factors during the pendency of the violation -there was a documented key system to track key access to the outer gate; a background check required for gate access; there was a procedure in place for tracking and revoking swipe card access; the keys at issue were used only in the event that the swipe card system was not functioning; these keys were unidentifiable could not provide gate access. Also, the registered entity had alarms in place and there were no incidents related to the lack of proper documentation and revocation of the keys during the violation period.

Mitigation of the violation required the installation of a new system for PSP substation access, and the creation of a new procedure to monitor access to the keys.

The Regional Entity evaluated the registered entity's compliance program and determined that it included preventive and corrective processes and procedures, internal controls and culture of compliance.

More than one violation involved in Settlement Agreement, related to the same set of facts.

Example 2

CIP-005-1 R2.1and R2.2

The facts and circumstances warrant a SNOP treatment because the risk to the BPS was moderate and not appropriate for a FFT treatment.

The risk was moderate because:

The registered entity did not have strong organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to its ESPs. This was evidenced by the fact registered entity did not require explicit access permissions (deny by default) and did not make sure that the access point only enables ports and services required for operations and monitoring. As a result, the registered entity exposed its networks to the possibility of unauthorized cyber access for a period of 9 and a half months.

There were mitigating factors during the pendency of the violation that reduced the risk to moderate: the registered entity had firewall rules that did limit access to trusted networks and only allowed non-interactive ports and services as the interactive ports were blocked. In addition only three employees had access to the firewall rule set and configuration files. Also, the registered entity's had mechanisms in place that led to the ultimate discovery of the violation.

More than one violation involved in Settlement Agreement, related to the same set of facts.

Mitigation of this violation required the changes in the registered entity's policy rules and procedures and additional training to relevant personnel.

The Regional Entity did not consider the registered entity's internal compliance plan (ICP) to be a mitigating factor in the penalty determination and considered it a neutral factor.

Example 3

CIP-006-1 R1.8

Reasons for SNOP treatment:

Risk to the reliability of the BPS: Minimal

The instances of noncompliance included several actions: failure to identify two CAs as CAs; failure to afford protective measures described under CIP-005-1 R2, CIP-007-1 R2, R3, R5 and R8, and CIP-009-1 R5 to three CAs; and failure to afford two protective measures to nine CAs.

There were mitigating factors during the pendency of the violation- nine of the twelve devices in scope were identified as CAs provisioning access control and monitoring. Even CAs that were not identified as access points, were equipped with protections that limited access. The registered entity's PSPs are dedicated to a specific network, which operates in complete isolation, and the PACM network itself is physically and electronically isolated, and access to it is controlled and monitored.

Mitigation of this violation required the changes in the registered entity's policy rules and procedures, implementation of new protective measures and incorporation all PACM assets used in the access control and monitoring of the PSP into the existing program for CCAs.

The registered entity's compliance program included preventive and corrective processes and procedures, internal controls and culture of compliance.

Example 4

CIP-006-1 R2

The facts and circumstances warrant a SNOP treatment because the risk to the BPS was moderate and not appropriate for a FFT treatment.

The risk was moderate because:

The instances of noncompliance included several actions. The registered entity failed to fully implement operational and procedural controls to manage physical access at all access points to six of its PSPs. As a result, one key could not be accounted for, some doors for the PSPs could be operated with a master key, and the physical key locks on these doors were not disabled, thus potentially exposing six PSPs to unauthorized physical access for a period ranging from 26 to 45 days. Further, the Regional Entity determined that in the worst case scenario, the devices within the PSPs could have been compromised to trip the two units at issue.

There were mitigating factors during the pendency of the violation- the assets were located inside a secured facility with armed guards, and these devices could not be remotely accessed.

Mitigation of this violation required the registered entity to change its procedures to require guards in the rooms and manual logging of access to the rooms. The registered entity also installed card readers and special key locks and disabled access to the doors at issue.

More than one violation involved in Settlement Agreement, related to the same set of facts.

The registered entity's ICP was not a mitigating factor in the penalty determination and was considered a neutral factor.

Answer Key OPS and Planning FFT Examples

Example 1

PRC-005-1 R1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

The issue was in documenting the testing intervals and the basis for intervals for the devices in question and not in the actual testing of the devices.

There were mitigating factors during the pendency of the issue- the registered entity was testing and monitoring the protection system devices in question through its SCADA system, and was also testing its batteries according to the intervals in its plan, testing its voltage and current sensing devices simultaneously with its relays, and routinely inspecting its substations, which includes checks of these devices. The registered entity was also monitoring its associated communication systems through its SCADA system, among other actions to mitigate the risk to the BPS.

Mitigation was completed by updating the registered entity's procedures, development of testing forms and conducting training on the revised procedures.

Example 2

FAC-008-1 R1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

The issue presented a documentation problem because the facilities rating methodology (FRM) did not address some of the devices, as required by this Standard.

There were mitigating factors during the pendency of the issue - the Ratings were developed during the design of the Facility and the final commissioning of the plant; the registered entity was operating its Facility as per the manufacturer's specifications; upon commissioning, it was determined that the turbines were the most limiting equipment and the registered entity's equipment and Ratings have not changed since commissioning.

Mitigation was completed by confirming the previous FRM and documenting and cataloging the methodology of major BPS equipment.

Example 3

FAC-009-1 R1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue- the generator interconnection transmission line that was not included in the implementation of the FRM was not the most limiting element of the Facility; proper coordination occurred between registered entity and the other registered entity; relay settings were reviewed and no need for modification was found; and the TOP, RC and PA, BA, RC were being informed of the line’s rating and status during the issue period.

Mitigation was completed by updating the Facility rating and providing the updated rating to the TOP, RC , and PA. the RC

Example 4

VAR-002-1.1aR3

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue- the unit maintained its voltage schedule; and the incident involved only one unit out of three units at the 500 MW facility.

The issue was limited in duration as it lasted only four hours.

Mitigation was completed by adding additional measures to prevent future occurrences and training plant operators on compliance with this Standard.

Example 5

EOP-005-1 R1

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

The issue presented a documentation problem because the registered entity did not have evidence that several system operators received System Restoration training but the operators participated in training and were familiar with system restoration.

There were mitigating factors during the pendency of the issue- system operators had performed multiple system restoration training simulations in the past and following the issue period.

Mitigation was completed by revising its procedure to include requirements for system operator training and documentation.

Example 6

PRC-008-0 R2

Reasons for FFT treatment:

This issue presented a minimal risk to the BPS at the time the issue occurred.

There were mitigating factors during the pendency of the issue- the size of the registered entity and the fact that it the registered entity had only 2 interconnection points to the BPS reduced the risk to minimal. Also, maintenance and testing was missed for only 2 devices.

Mitigation was completed by performing an inventory, identifying all equipment that was part of the issue, completed maintenance and testing, adjusted its maintenance and testing policy.

Answer Key OPS and Planning SNOP Examples

Example 1

PRC-005-1 R2

Reasons for SNOP treatment:

Risk to the reliability of the BPS: Minimal

The scope of the violation was broad, involving 47% of the registered entity's Protection System devices.

The violation was the result of a lack of a comprehensive formal program for the scheduling and documentation of all the Protection System maintenance and testing at the registered entity's facility. Instead, the registered entity relied on informal and undocumented program activity.

There was a prior history of noncompliance with this Standard.

The duration of the violation was for several years, from 2007 to 2011 and the internal compliance controls did not lead to discovery of the violation.

There were mitigating factors during the pendency of the violation- the registered entity used the manufacturer's maintenance and testing procedures and intervals; conducted visual inspections and voltage checks.

More than one violation involved in Settlement Agreement, related to the same set of facts.

Mitigation of this violation required changes in the registered entity's policy rules and procedures and additional training of relevant personnel.

Example 2

VAR-002-1.1b R3

Risk to the reliability of the BPS: Minimal

The violation lasted for a long period of time from August 2, 2007 until January 12, 2011 and the registered entity's internal compliance controls (or lack of such controls) did not lead to discovery of the violation.

There were mitigating factors during the pendency of the violation - the STG was operated in the correct mode; the output of the plant was always within the operating parameters; the operating personnel followed all directives given by BPA when deviations to the voltage schedule were required; the size of the plant was 249 MW with an annual operation of less than 50 %.

More than one violation involved in Settlement Agreement, related to same set of facts.

Mitigation of this violation required changes in the registered entity's policy rules and procedures and additional training of relevant personnel.

Example 3

FAC-008-1 R1

Risk to the reliability of the BPS: Minimal

The violation involves more than one act of noncompliance: the registered entity did not have a FRM prior to August 27, 2007, and once it adopted an FRM, did not address all necessary equipment; and the registered entity's FRM did not cover its transmission equipment.

There were mitigating factors during the pendency of the violation - the FRM was designed to reflect the most limiting element; the revised Facility Rating did not change; and the registered entity attested that the Facilities were rated based on manufacturer's ratings and the units had been operated in accordance with those Ratings.

The violation lasted for several years from 2007 to 2011; and its internal compliance controls (or lack of such controls) did not lead to discovery of the violation.

The registered entity's ICP did not lead to the discovery of the violation because it was implemented later. Therefore, the Regional Entity considered it a neutral factor.

More than one violation involved in Settlement Agreement, related to same set of facts.

Mitigation of this violation required changes in the registered entity's policy rules and procedures.

Example 4

PER-003-0 R1

The facts and circumstances warrant a SNOP treatment because the risk to the BPS was moderate and not appropriate for a FFT treatment.

The risk was moderate because:

The registered entity failed to follow its Implementation Plan and make sure that its operators were NERC-certified by a specific deadline date. In addition, the violation was discovered through an audit, indicating lack of internal compliance controls that could lead to discovery of the violation. Failure to staff with NERC-certified operators who are sufficiently trained to operate the BPS presented a risk of a potential failure of the BPS.

There were mitigating factors during the pendency of the violation – the operators had received extensive training and demonstrated competency in their jobs' duties. The operators were enrolled in a training program and had access to tutorials and other materials providing training. The registered entity had an internal policy in effect providing the operators with a timeline for completing the certification process.

Mitigation of this violation required delegation of specific TOP activities to a registered TOP which provided NERC certified operators to operate the registered entity's transmission system. In addition the registered entity provided resources to the operators to pass certification, changed some of its policy rules and procedures and added additional personnel.

The Regional Entity evaluated the registered entity's compliance program and determined that it included corrective processes and procedures, internal controls and culture of compliance.

Example 5

COM-002-2 R2

The facts and circumstances warrant a SNOP treatment because the risk to the BPS was moderate and not appropriate for a FFT treatment.

The risk was moderate because:

The violation was related to real-time operations of the BPS. The switching directives could have been performed incorrectly which would have resulted in delays in proper restoration or additional equipment being forced out. Also, the communication at issue was given during a period of restoration of equipment, and therefore took place under normal conditions rather than during a time of high stress, system instability, or system emergency, indicating that the violation presented a risk to the reliability of the BPS during emergencies as well.

There were mitigating factors during the pendency of the violation- the directive which was given in an improper manner was nonetheless carried out by the recipient in the correct manner and thus did not cause any additional risk or result in an incident.

The Regional Entity evaluated the registered entity's compliance program and determined that it included preventive and corrective processes and procedures, internal controls and culture of compliance.

Mitigation of this violation required changes in the registered entity's policy rules and procedures and training of relevant personnel.

Example 6

TOP-004-2 R1

Risk to the reliability of the BPS: Minimal

A failed static wire resulted in the outage of two 138 kV transmission lines, and the system operator initiated a load shed of the registered entity's local load (approximately 135 MW) for approximately one hour to resolve what appeared to be a transformer overload. However, tests performed after the event indicated that the autotransformer in question had been rated conservatively and was not overloaded, had not been damaged and was not at risk of failure.

There were mitigating factors during the pendency of the violation- the manual load shed performed to correct the exceedance affected only local load; no instability, uncontrolled separation, or cascading outages resulting from the loss of the 230/138 kV autotransformer

could have occurred; the autotransformer was never actually overloaded because it had been rated conservatively.

The Regional Entity evaluated the registered entity's compliance program and determined that it included preventive and corrective processes and procedures, internal controls and culture of compliance.

Mitigation of this violation required changes in the registered entity's policy rules and procedures and training of relevant personnel.

Exhibit D

Compliance Enforcement Initiative Training for Auditors and Investigators

September 20, 2012 - Atlanta, GA

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Enforcement Initiative Training for Auditors and Investigators

Atlanta
September 20, 2012

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Learning Objectives

- Describe the characteristics of the Find, Fix, Track and Report (FFT) mechanism
- Describe the FFT process
- Discuss the roles and responsibilities of Compliance Staff, Enforcement Staff, and Industry
- Explain conditions that would and would not qualify for FFT treatment
- Review examples of appropriate FFT risk assessments
- Discuss use of FFT vs. Notice of Penalty (NOP) treatment

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda

- Overview of the Compliance Enforcement Initiative (CEI)
- Characteristics of FFT Remediated Issues and NOP Violations
- Contents of an FFT
- FFT Process
- Examples of Identifying Critical Infrastructure Protection (CIP) FFTs and Spreadsheet NOPs (SNOPs)
- Examples of Identifying Operations and Planning FFTs and SNOPs
- Discussion of Exercises
- Ongoing CEI Implementation and Development

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Overview of the Compliance Enforcement Initiative

RELIABILITY | ACCOUNTABILITY

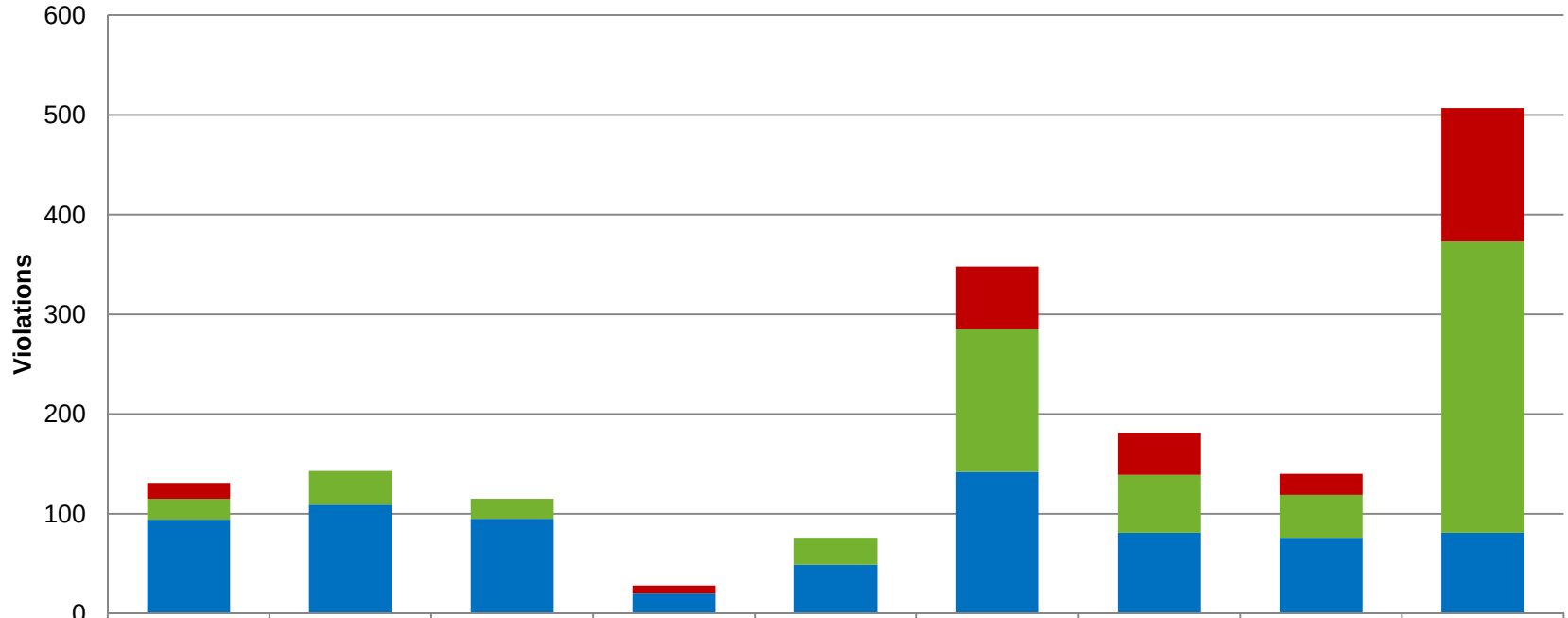



Development History

- Increasing emphasis on risk-based enforcement
  - Greater efficiency
  - Focus on greatest risks to Bulk Power System (BPS) reliability
- Petition for FFT mechanism approval and first batch of FFTs filed September 30, 2011
- FERC issues order on March 15, 2012 approving FFT program

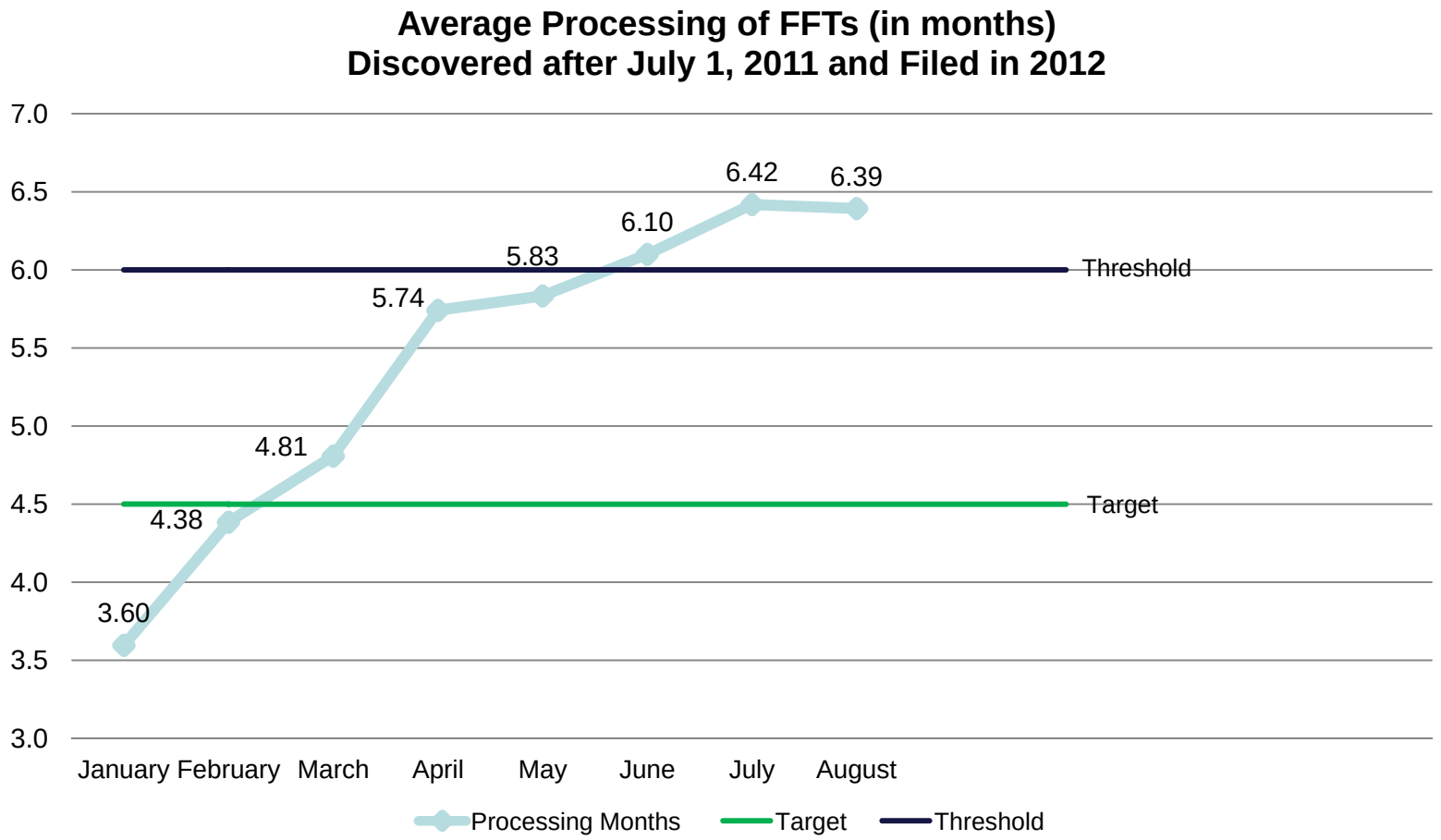
Filed FFTs/SNOPs/NOPs by Region

FFTs/SNOPs/NOPs
By Region
Filed from September 1, 2011 to August 31, 2012



	SERC	FRCC	MRO	NCEA	NPCC	RFC	SPP	TRE	WECC
NOP	16			8		63	42	21	134
SNOP	21	34	20		27	143	58	43	292
FFT	94	109	95	20	49	142	81	76	81

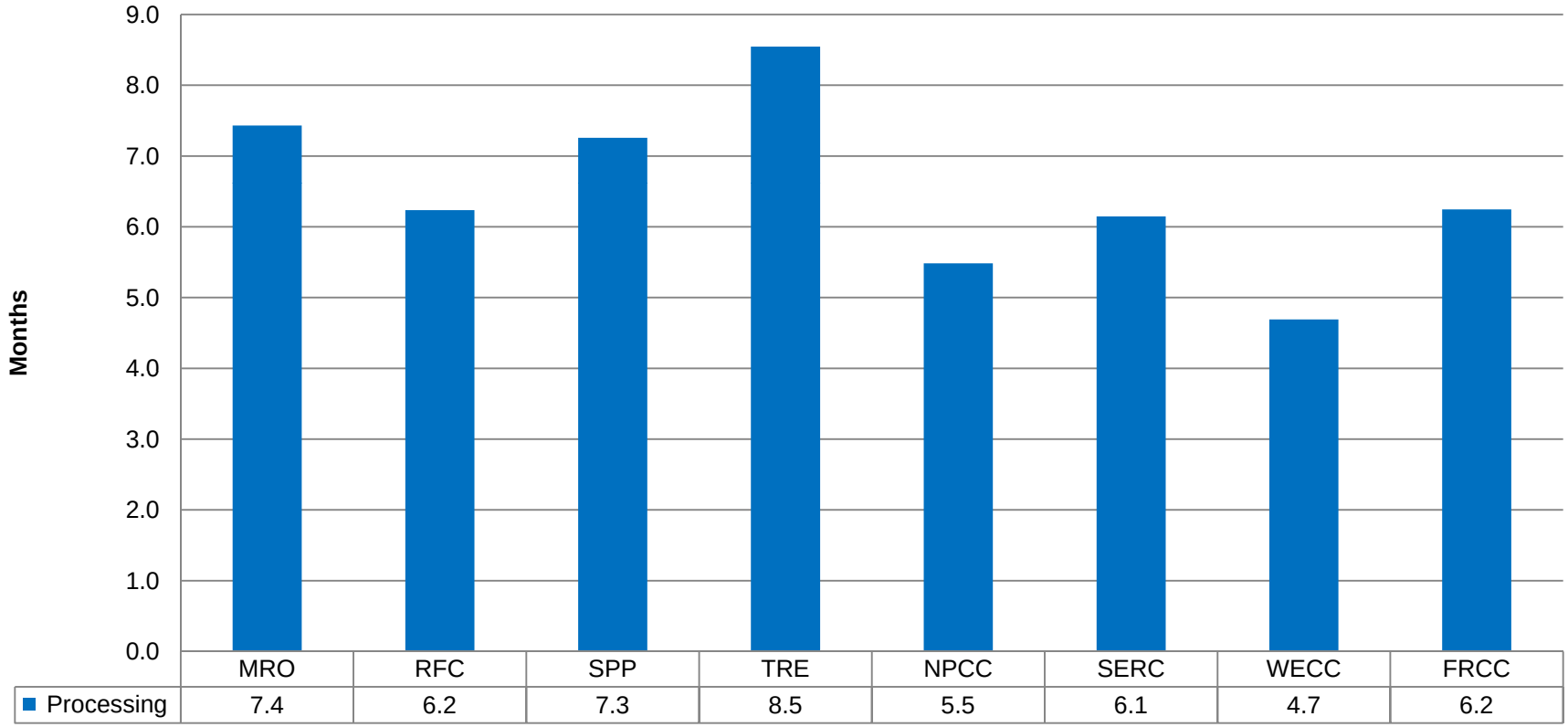
FFT Processing Time



Data and Trends

Avg. Number of Months for FFT Processing From Discovery to Filing

Violations Discovered after July 1, 2011
Filed September 2011 to August 31, 2012



	MRO	RFC	SPP	TRE	NPCC	SERC	WECC	FRCC
Processing	7.4	6.2	7.3	8.5	5.5	6.1	4.7	6.2

Possible Improvement

- Continue to focus on high risk issues, but for minimal risk issues receiving FFT treatment:
  - Regional Entities should improve their internal processes
  - Registered entities encouraged to improve processing times through more efficient completion of mitigation and certification

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Characteristics of FFT Remediated Issues and NOP Violations

RELIABILITY | ACCOUNTABILITY




FFT Basics

- Underlying noncompliance matter is referred to as "remediated issue" and not a "violation"
- Only applicable to issues posing minimal risk to the BPS
- FFTs are not subject to penalties
- FFTs become part of entities' compliance histories

FFT Basics

- Mitigation activities need to be completed and certified—by an officer or equivalent—and no formal mitigation plan is required
  - In general, mitigation activities for minimal risk violations should take less time to complete than more serious violations
- NERC does not require the full record in order to process an FFT; uses abbreviated spreadsheet filing format while region keeps record
- FFTs processed on rolling basis; NERC internal review is shorter

Evaluation Criteria

- Underlying facts and circumstances (i.e., what happened, why, where and when)
- Relevant Reliability Standard
- Applicable Violation Risk Factor (VRF)
- Violation Severity Level (VSL)

Evaluation Criteria

- The potential and actual level of risk to reliability, including mitigating factors during pendency of the Possible Violation
- The registered entity's compliance program, including preventive and corrective processes and procedures, internal controls and culture of compliance
- The registered entity's compliance history

FERC Guidance on Risk Assessment

- No adverse impact ≠ minimal risk
  - However, other factors may lead to minimal risk
- Do not base risk assessments on assumptions
  - Stick to the facts
- Programmatic shortcomings ≠ minimal risk

FERC Guidance on Risk Assessments

- Assess risk based on facts at the time of the possible violation
- Existing processes and contemporaneous actions can make actual risk < potential risk
  - Potential risk = possible outcomes of noncompliance without regard to specific facts and circumstances of the violation
  - Actual risk = the outcomes based on the specific facts and circumstances of the violation, *e.g.*, compensating measures, characteristics of entity, *etc*.

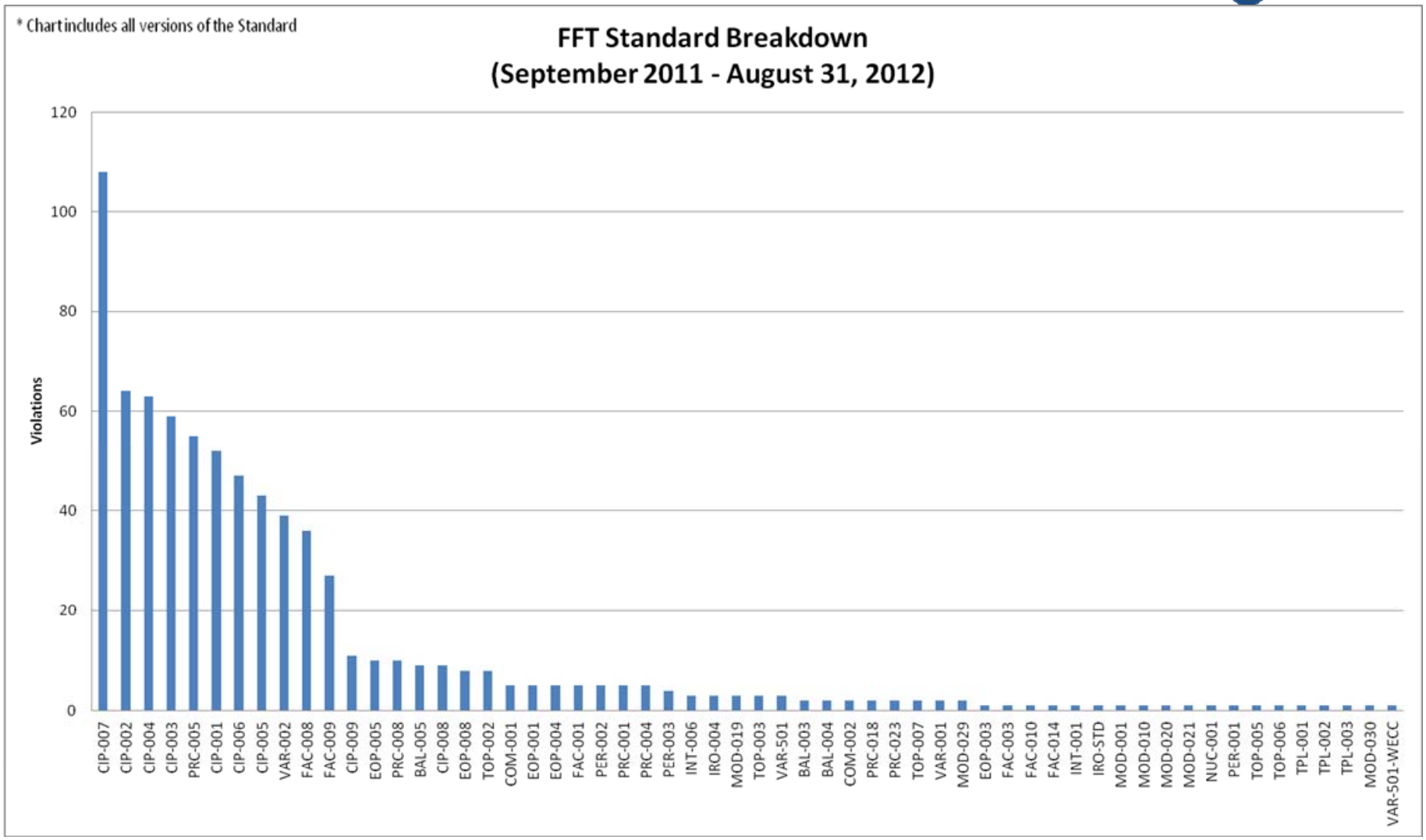
Compliance History and FFT Treatment

- Repeat issues are eligible for FFT treatment, provided that they pose only a minimal risk to the reliability of the BPS
- Factors include (a) timing and nature of violations/issues, and (b) method of discovery
- Factors weighing against FFT Treatment
  - Registered entity's compliance history is indicative of broader concerns
  - Prior remediated issue was subsequently found not to have been mitigated
  - Material misrepresentations about the nature and scope of a prior issue

FFTs and the Big Picture

- Separating out individual violations for FFT treatment from others found in an Audit can be appropriate
  - The violations need to meet FFT criteria
  - Need to capture full scope of risk for the violations
    - Violations stemming from common shortcomings should be assessed and treated together

Reliability Standards Receiving FFT Treatment



Explanation of Frequency

- Late-filed technical feasibility exceptions (TFEs) contribute to the frequency of CIP-007
- Documentation issues predominate for CIP-002, -003 and -004, as well as FAC-008 and -009
- Small number of missed devices and redundant protections for PRC-005

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Contents of an FFT

RELIABILITY | ACCOUNTABILITY




Anatomy of an FFT

- Describe the Remediated Issue
  - Facts associated with the violation (i.e., scope, duration, location, and specification of noncompliance with the requirement)
- Describe the Risk Assessment
  - Risk must be minimal
  - Address potential and actual risk
  - Factors that mitigated the potential risk
- Describe the Status of Mitigation Activity
  - Complete and certify mitigation activities
  - Remediate noncompliance and prevent recurrence

FFT Disqualifiers

- Loss of customer load
- Pattern of noncompliance
- Greater than minimal risk
- Failure to remediate
- Closely linked to other violations

FFTs Recast as SNOPs

- For several registered entities, issues that could have been FFTs have been subject to financial penalties
  - History of noncompliance related to the same requirement
  - Deficiencies in internal compliance programs
  - Closely linked to other violations

Common Issues with Processing FFTs

- Insufficient facts to support the issue
- Insufficient explanation of minimal risk
  - Mitigating factors during pendency of noncompliance
- Timeliness of mitigation activity completion
- Registered entity's timeliness of certification of completion

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FFT Process

RELIABILITY | ACCOUNTABILITY




Violation Processing Tracks

- If a potential noncompliance is not a Possible Violation, then it is dismissed
- Possible Violations considered on their merits
- Minimal risk issues considered for FFT treatment
- Minimal or moderate risk issues may be subject to penalty and treated in SNOPs
- Full NOP used for higher-risk violations and cases involving large number of violations or financial penalties

FFT Process

- Identification of Possible Violation
- Assessment of risk
- Evaluation of mitigating activities, if any have occurred
- Consideration of registered entity and compliance history
- Compliance Staff can make recommendation of FFT treatment
- Regional entity decision to afford FFT treatment

FFT Process

- Regional Entity drafts FFT spreadsheet and sends to NERC
- NERC evaluates FFTs submitted by Regional Entity and informs Regional Entity of FFT approval or rejection
- Regional Entity sends Opt-out letter to registered entity
- NERC prepares FFT for filing with FERC
- If registered entity certifies completion of mitigating activities and does not opt out, then NERC files the FFT with FERC
  - Verification is not a requirement for filing an FFT with FERC
- With no further action by FERC, FFT is closed after 60 days

Compliance Staff & the FFT Process

- Compliance Staff can make FFT recommendations to Enforcement Staff for issues identified during an Audit or a Spot Check
  - Recommendations should be supported by spreadsheet that includes:
    - Description of the issue
    - Assessment of the risk
    - Listing of mitigating activities, if any at that point
- While not "fix in the field," Compliance Staff may still verify what the registered entity does to mitigate the potential noncompliance

Example of FFT Spreadsheet

The Searchable FFT Informational Filing Spreadsheet is based on remediated issues that were submitted for informational purposes only. In the event of a conflict between information on the Searchable FFT spreadsheet and filed FFTs, the filed FFTs govern.

Informational Filing Date Regional Entity Registered entity NCR Issue Tracking # Standard / Requirement	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
	On April 11, 2012, XXX as a Transmission Owner, self-reported an issue with PRC-005-1a R2. During an internal review of XXX's Protection System maintenance and testing program, maintenance for a single transmission substation battery bank was identified as having a completion date which was past the interval-based due date by four days. Maintenance on the battery bank at issue should have been completed on September 30, 2011 and was actually completed on October 4, 2011.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the batteries were continuously monitored and an alarm would have alerted personnel in case of a voltage issue or an open battery bank. Additionally, the battery bank was only four days overdue for testing and maintenance. When tested, the batteries were found to be fully functional.	To mitigate this issue, XXX tested and maintained the battery bank that was out of interval, and trained the contractor and XXX personnel on the procedure and necessity for on-time maintenance.

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

Compliance Staff and the Registered Entity

- Recommendations not expected to be shared with the registered entity during an audit or spot check
- When lobbied for FFT treatment, commit only to sharing the registered entity's information with Enforcement Staff
- Best practice is not to say either "Yes" or "No" to possible FFT treatment

FFT Drafting Considerations

- In explaining minimal risk CIP candidates, avoid:
  - Stating that firewalls alone are effective mitigating controls for CIP-002 or -007 violations
  - Using the phrase "all of the requirements" or "all of the systems were protected" or "all other systems were compliant" and specify what was and was not in place
  - Making general statements about risk by focusing on specific compensating or mitigating measures for the Critical Asset or Critical Cyber Asset in scope
- Document input from your technical Subject Matter Experts
- Be aware of potential indications of process failures

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Examples of CIP FFTs and SNOPs

RELIABILITY | ACCOUNTABILITY




CIP-007-1 R4.1

- **Issue:**
  - During an energy management system (EMS) replacement, a legacy EMS system did not receive virus updates as described in the registered entity's anti-virus (AV) process in order to comply with CIP 007 R4.1.
  - As a result the registered entity's legacy EMS was potentially exposed to viruses and malware for a 37-day period while the new EMS system was being implemented (which utilized a different AV software and was receiving the required updates).

CIP-007-1 R4.1

- **Risk Considerations:** The legacy EMS was disconnected from the serial remote terminal unit (RTU) paths and its ability to affect the bulk electric system operations was minimal.
  - The legacy EMS was still within the electronic security perimeter (ESP) during the violation period
- **Mitigating Activities:** The region relied upon entity attestation that ESP access, monitoring and other security controls remained in place during the violation period.

Reasons for FFT treatment

- **Risk Determination:**
  - Minimal
- **Key Factors:**
  - The EMS was no longer connected to the field devices after the switchover was made.
  - Logs, ports/services and account access logs were reviewed during the violation period to ensure that malicious activity did not occur.

Risk Statement

- **Risk Considerations**
  - 37-day exposure
  - Core EMS platforms were involved
  - AV software was up-to-date on new EMS
  - Legacy EMS had limited command and control capability
  - Entity attestation verifying that underlying risk or residual risk was effectively assessed and mitigated

CIP-006 R1.1

- During a Compliance Spot Check, the Regional Entity discovered that the registered entity, as a Balancing Authority, Generator Owner, Generator Operator, Load Serving Entity, Transmission Operator, Transmission Owner, Transmission Service Provider and Interchange Authority, failed to identify six of its physical access control system (PACS) Cyber Assets and to afford them the protection required by CIP-006 R2.2.
- This condition existed from July 1, 2009 to August 22, 2011.

Determination of Risk

- **Risk Determination:**
  - Moderate
- **Key Factors:**
  - 782-day exposure
  - Physical access to CCAs could be compromised
  - If physical access is breached, protections afforded to the CCAs by other CIP requirements are nullified

Mitigation Considerations

- **Risk Considerations:**
  - The six systems were not afforded the overarching protection of the registered entity's cyber security policy nor the required oversight of a senior manager.
  - The personnel with access to these six systems were not screened with a personnel risk assessment program.
  - The six systems were not protected with the required technical and procedural controls to allow only authorized electronic access.
  - The six systems were not being monitored as required.

Mitigation Considerations

- **Key Factors Continued:**
  - The six systems did not necessarily receive all of the physical access controls and monitoring required.
  - Did these six systems have test procedures?
  - Were their ports and services managed?
  - Did they receive timely patches?
  - Were their passwords complex and changed frequently?
- At a minimum, all of the above should be considered in the mitigation plan.

CIP-007-1 R1

- **Issue:** A failure to use appropriate test procedures to ensure that new CAs and significant changes to CAs within the ESP do not adversely affect existing cyber security controls.
  - The entity periodically utilized an intermediate AV server to download AV signature and security patch updates for the CAs within the ESP but failed to test the server each time it was reintroduced into the ESP.

CIP-007-1 R1

- **Risk Considerations:** The entity did not consider the AV server to be a "new" CA each time it reconnected to the ESP, and therefore could not demonstrate that appropriate test procedures had been followed.
- **Mitigating Activities:** The entity ceased the practice of updating AV signatures using a temporary intermediate AV server, revised the EMS AV signature update process, and reviewed and confirmed all EMS cyber assets are properly identified and protected.

Reasons for NOP treatment

- **Risk determination:** Substantial
- **Key factors:**
  - The intermediate AV server utilized by the registered entity was configured as a hardened, single-purpose device, thus reducing the risk of compromise by malware or other exploits. – How was the system hardened? Who verified?
  - The registered entity tested anti-malware signatures and security patch updates in a development environment prior to introduction to the ESP.
  - The intermediate AV server was not connected simultaneously to the ESP and the registered entity corporate network. This does not assure that exposure is mitigated to ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Identifying Operations and Planning FFTs and SNOPs

RELIABILITY | ACCOUNTABILITY




PRC-005-1 R2

- **Issue**: Failure to maintain and test transmission Protection System devices in accordance with the defined intervals in Protection System maintenance and testing program.
  - Failure to maintain and test 56 devices out of 861 total devices, or approximately 6.5%.
- **Risk Considerations**: The devices at issue were continuously monitored via a supervisory control and data acquisition system.
- **Mitigating Activities**: The entity completed inventory of each BPS device, developed a "catch-up" maintenance and testing plan and schedule, trained its technicians, and notified contractor personnel regarding revisions to the program.

Reasons for FFT treatment

- **Risk Determination**: Minimal
- **Key Factors**:
  - Less than 7% of devices were not tested, equating to a Lower VSL
  - The devices at issue were continuously monitored via a supervisory control and data acquisition system.
  - Size of the registered entity - annual peak of less than 600 MW in 2009

Risk Statement

- **Risk Considerations:**
  - Relays were being continuously monitored via supervisory control and data acquisition (SCADA) system
  - 56 devices out of 861 total devices involved, or approximately 6.5%
  - Size of registered entity's generation and transmission facilities

PRC-005-1 R1.1

- **Issue:** Documents of the registered entity's relay maintenance and testing program for the BPS did not show maintenance and testing intervals for its Current Transformer (CT) and Potential Transformer (PT) devices.
- **Risk Considerations**: The 70 total CTs and PTs at issue comprised fewer than 25% of the 408 applicable Protection System devices.
- **Mitigating Activities**: The registered entity revised its Protection System maintenance and testing program to include last testing date and next testing date for CT and PT devices.

Reasons for SNOP treatment

- **Risk Determination**: Moderate
- **Key Factors**:
  - Duration over several years
  - During the pendency of the violation, the registered entity verified the integrity of the CT and PT devices by performing testing periodically as per the registered entity's maintenance documents
  - The registered entity employs back-up relaying providing backup protection should the primary systems fail

Risk Statement

- **Risk Considerations:**
  - The registered entity employs back-up relaying providing backup protection should the primary systems fail.
  - The result of the CT and PT devices tested satisfactorily.
  - The duration spans over several years.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comparing Results and Discussing Common Challenges

RELIABILITY | ACCOUNTABILITY




Exercises

- Review facts, circumstances, and risks of the noncompliance
- Assess the risk of the noncompliance, including categorizing as minimal or moderate risk
  - Compose the risk statement
- Recommend appropriate disposition track
  - FFT or NOP

Discussion of Exercises

- Enough information to make a decision?
  - What information is most useful? Least useful?
  - What more do you need to know to come to a recommendation for disposition?
    - Are you able to provide that information to your Regional Entity?
- What information most affects the risk determination?
- What types of violations merit imposition of penalties?
- How confident were you in your recommendation of the disposition track?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Ongoing CEI Implementation and Development

RELIABILITY | ACCOUNTABILITY




CEI Ongoing Implementation

- Third Quarter 2012
  - September compliance enforcement authority (CEA) Staff workshop and training course
  - Begin random sampling of FFTs already filed with FERC
- Fourth Quarter 2012
  - Online webinar courses for CEA staff
  - All CEA compliance monitoring staff complete required training course
- 2013
  - Propose additional CEI improvements

Random Sampling

- Include results of sampling in 12-month status report to FERC (March 15, 2013)
- Begin sampling in September or October to have results by end of 2012
- Random selection of FFTs to survey using accepted sampling methodology
  - Ensures that reliability issues have been fixed as certified by the registered entity and that the issue has not recurred
  - Validates risk assessment and that penalty was not necessary
  - Monitors program and identify improvements rather than reopen FFTs or second-guess the Regional Entities
- FERC has announced a similar intent to survey a random sample of FFTs

CEI Pathway Forward

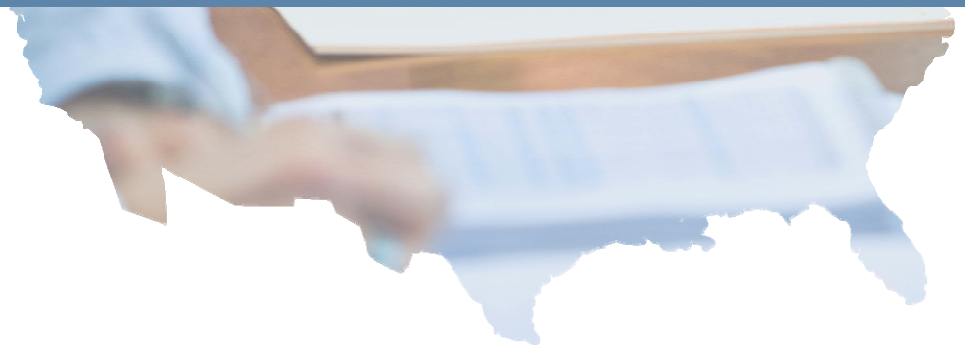
- NERC and the Regional Entities commenced development and planning
- The process will include:
  - Whitepaper
  - Pilot test of plan elements
  - Communication with Industry and FERC
  - Propose comprehensive approach in March 2013 CEI compliance filing

Conclusion

- FFT is a useful tool for handling minimal risk issues that do not require imposition of a penalty
  - Not just $0 penalty violations
- Gather as much information as possible about a noncompliance in order to assess the risk fully and recommend a disposition track
- Collaborate with Regional Enforcement Staff on developing and packaging information to support recommendations and make processing of non-compliances more efficient

Questions

Questions and Answers



Contact Information

Ken Lotterhos
Associate General Counsel &
Director of Enforcement
(202) 400-3009
ken.lotterhos@nerc.net

Ed Kichline
Mgr. of Enforcement Processing
(202) 400-3025
ed.kichline@nerc.net

Exhibit E

Compliance Enforcement Initiative Training for Industry

September 21, 2012 - Atlanta, GA

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Enforcement Initiative Training for Industry

Atlanta
September 21, 2012

RELIABILITY | ACCOUNTABILITY




NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Learning Objectives

- Describe the characteristics of the Find, Fix, Track and Report (FFT) mechanism
- Describe the FFT process
- Discuss the roles and responsibilities of Compliance Staff, Enforcement Staff, and Industry
- Explain conditions that would and would not qualify for FFT treatment
- Review examples of appropriate FFT risk assessments
- Discuss use of FFT vs. Notice of Penalty (NOP) treatment

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda

- Overview of the Compliance Enforcement Initiative (CEI)
- Characteristics of FFT Remediated Issues and NOP Violations
- Contents of an FFT
- FFT Process
- Examples of Identifying Critical Infrastructure Protection (CIP) FFTs and Spreadsheet NOPs (SNOPs)
- Examples of Identifying Operations and Planning FFTs and SNOPs
- Discussion of Exercises
- Ongoing CEI Implementation and Development

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Overview of the Compliance Enforcement Initiative

RELIABILITY | ACCOUNTABILITY

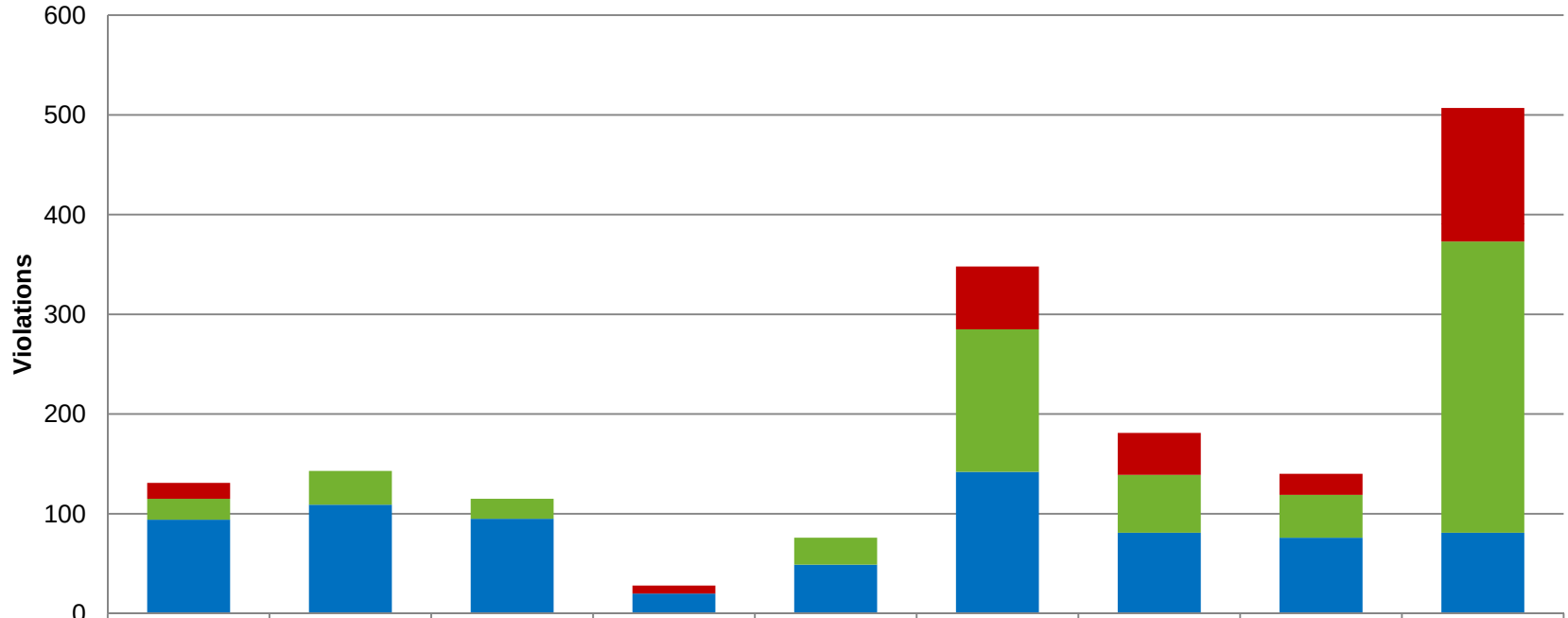



Development History

- Increasing emphasis on risk-based enforcement
  - Greater efficiency
  - Focus on greatest risks to Bulk Power System (BPS) reliability
- Petition for FFT mechanism approval and first batch of FFTs filed September 30, 2011
- FERC issues order on March 15, 2012 approving FFT program

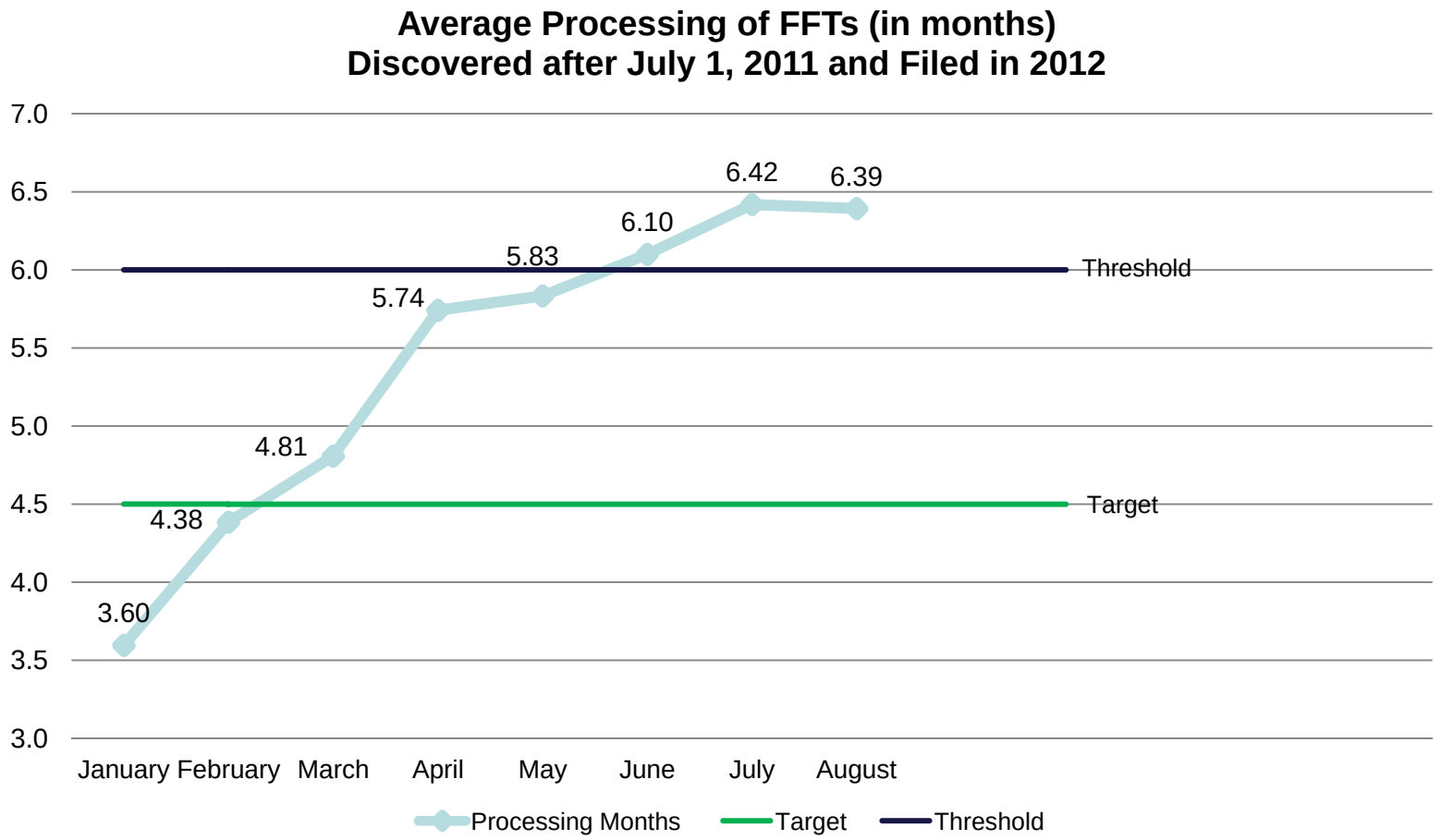
Filed FFTs/SNOPs/NOPs by Region

FFTs/SNOPs/NOPs
By Region
Filed from September 1, 2011 to August 31, 2012



	SERC	FRCC	MRO	NCEA	NPCC	RFC	SPP	TRE	WECC
NOP	16			8		63	42	21	134
SNOP	21	34	20		27	143	58	43	292
FFT	94	109	95	20	49	142	81	76	81

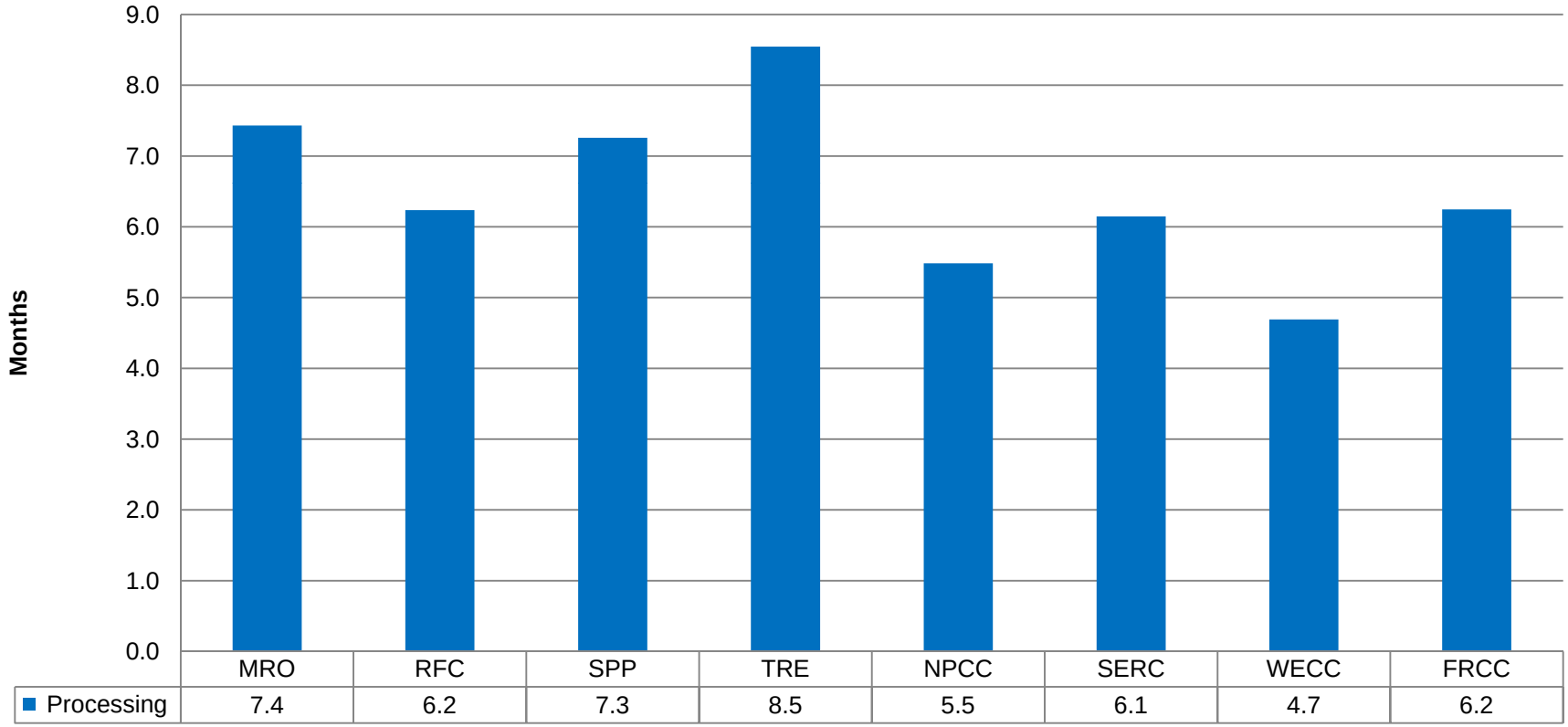
FFT Processing Time



Data and Trends

Avg. Number of Months for FFT Processing From Discovery to Filing

Violations Discovered after July 1, 2011
Filed September 2011 to August 31, 2012



	MRO	RFC	SPP	TRE	NPCC	SERC	WECC	FRCC
Processing	7.4	6.2	7.3	8.5	5.5	6.1	4.7	6.2

Possible Improvement

- Continue to focus on high risk issues, but for minimal risk issues receiving FFT treatment:
  - Regions to improve their internal processes
  - Registered entities encouraged to improve processing times through more efficient completion of mitigation and certification

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Characteristics of FFT Remediated Issues and NOP Violations

RELIABILITY | ACCOUNTABILITY




FFT Basics

- Underlying noncompliance matter is referred to as "remediated issue" and not a "violation"
- Only applicable to issues posing minimal risk to the BPS
- FFTs are not subject to penalties
- FFTs become part of entities' compliance histories
- Mitigation activities need to be completed and certified—by an officer or equivalent—and no formal mitigation plan is required
  - In general, mitigation activities for minimal risk violations should take less time to complete than more serious violations

FFT Basics

- NERC does not require the full record in order to process an FFT; uses abbreviated spreadsheet filing format while region keeps record
- FFTs processed on rolling basis; NERC internal review is shorter

Evaluation Criteria

- Underlying facts and circumstances (i.e., what happened, why, where and when)
- Relevant Reliability Standard
- Applicable Violation Risk Factor (VRF)
- Violation Severity Level (VSL)

Evaluation Criteria

- The potential and actual level of risk to reliability, including mitigating factors during pendency of the Possible Violation
- The registered entity's compliance program, including preventive and corrective processes and procedures, internal controls and culture of compliance
- The registered entity's compliance history

FERC Guidance on Risk Assessment

- No adverse impact ≠ minimal risk
  - However, other factors may lead to minimal risk
- Do not base risk assessments on assumptions
  - Stick to the facts
- Programmatic shortcomings ≠ minimal risk

FERC Guidance on Risk Assessments

- Assess risk based on facts at the time of the possible violation
- Existing processes and contemporaneous actions can make actual risk < potential risk
  - Potential risk = possible outcomes of noncompliance without regard to specific facts and circumstances of the violation
  - Actual risk = the outcomes based on the specific facts and circumstances of the violation, *e.g.*, compensating measures, characteristics of entity, *etc*.

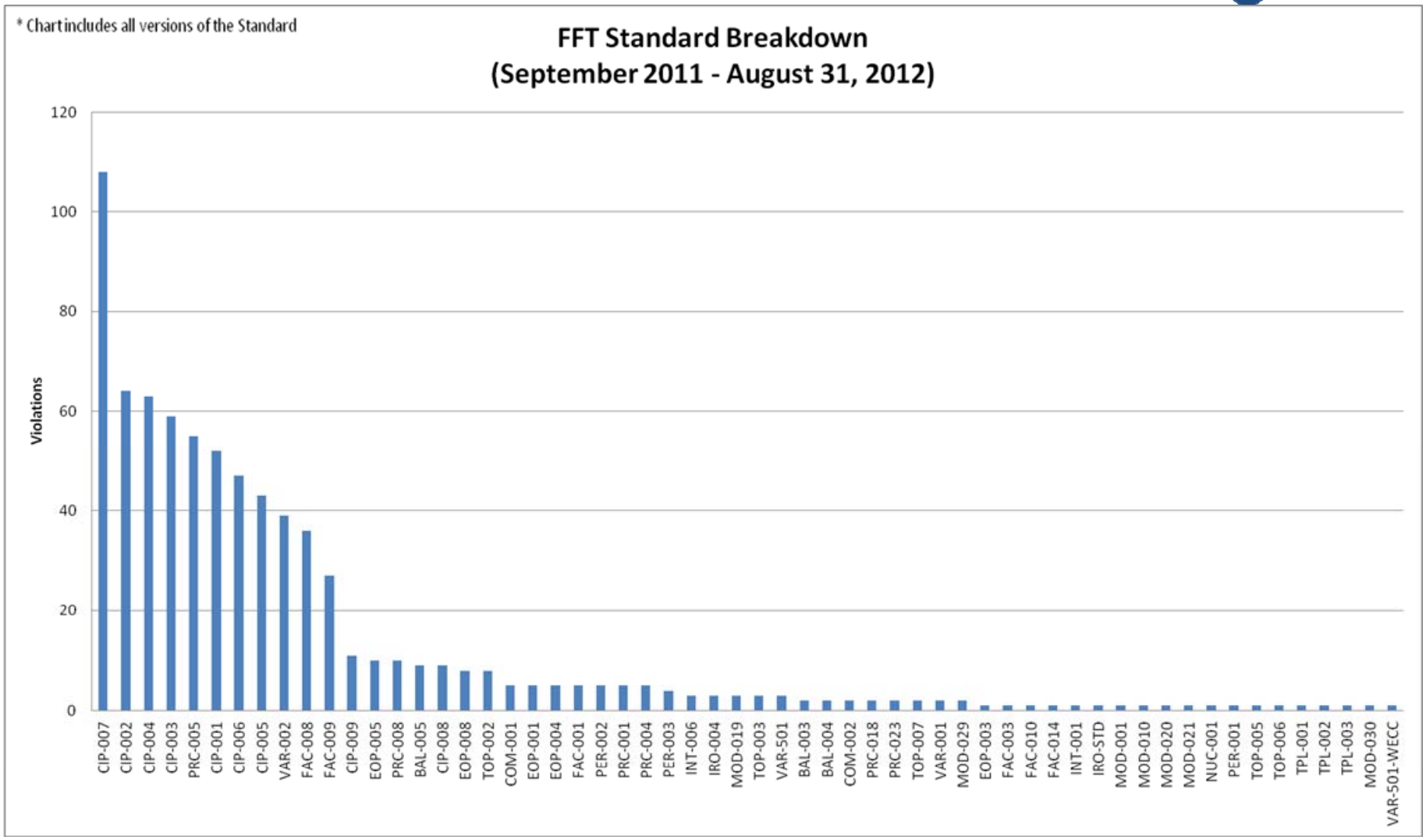
Compliance History as a Factor in Considering FFT Treatment

- Repeat issues are eligible for FFT treatment, provided that they pose only a minimal risk to the reliability of the BPS
- Factors include (a) timing and nature of violations/issues, and (b) method of discovery
- Issues that would NOT be afforded FFT Treatment
  - Where entity's compliance history is indicative of broader concerns
  - Where prior remediated issue was subsequently found not to have been mitigated
  - Cases involving material misrepresentations about the nature and scope of the prior issue

FFTs and the Big Picture

- Separating out individual violations for FFT treatment from others found in an Audit can be appropriate
  - These violations need to meet FFT criteria
  - Need to capture full scope of risk for the violations
    - Violations stemming from common shortcomings should be assessed and treated together

Reliability Standards Receiving FFT Treatment



Explanation of Frequency

- Late-filed technical feasibility exceptions (TFEs) contribute to the frequency of CIP-007
- Documentation issues predominate for CIP-002, -003 and -004, as well as FAC-008 and -009
- Small number of missed devices and redundant protections for PRC-005

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Contents of an FFT

RELIABILITY | ACCOUNTABILITY




Anatomy of an FFT

- Description of Remediated Issue
  - Facts associated with the violation, including scope, duration, location, and specification of noncompliance with the requirement
- Description of the Risk Assessment
  - Risk must be minimal
  - Address potential and actual risk
  - Factors that mitigated the potential risk
- Description and Status of Mitigation Activity
  - Mitigation activities must be completed and certified
  - Remediating the noncompliance and preventing recurrence

FFT Disqualifiers

- Loss of customer load
- Pattern of noncompliance
- Greater than minimal risk
- Failure to remediate
- Closely linked to other violations

FFTs Recast as SNOPs

- For several registered entities, issues that could have been FFTs have been subject to financial penalties
  - History of noncompliance related to the same requirement
  - Deficiencies in internal compliance programs
  - Closely linked to other violations

Common Issues with Processing FFTs

- Insufficient facts to support the issue
- Insufficient explanation of minimal risk
  - Mitigating factors during pendency of noncompliance
- Timeliness of mitigation activity completion
- Registered entity's timeliness of certification of completion

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FFT Process

RELIABILITY | ACCOUNTABILITY




Violation Processing Tracks

- If a potential noncompliance is not a Possible Violation, then it is dismissed
- Possible Violations considered on their merits
- Minimal risk issues considered for FFT treatment
- Minimal or moderate risk issues may be subject to penalty and treated in SNOPs
- Full NOP used for higher-risk violations and cases involving large number of violations or financial penalties

FFT Process

- Identification of Possible Violation
- Assessment of risk
- Evaluation of mitigating activities, if any have occurred
- Consideration of registered entity and compliance history
- Compliance Staff can make recommendation of FFT treatment
- Regional entity decision to afford FFT treatment

FFT Process

- Regional Entity drafts FFT spreadsheet and sends to NERC
- NERC evaluates FFTs submitted by Regional Entity and informs Regional Entity of FFT approval or rejection
- Regional Entity sends Opt-out letter to registered entity
- NERC prepares FFT for filing with FERC
- If registered entity certifies completion of mitigating activities and does not opt out, then NERC files the FFT with FERC
  - Verification is not a requirement for filing an FFT with FERC
- With no further action by FERC, FFT is closed after 60 days

Compliance Staff & the FFT Process

- Compliance Staff can make FFT recommendations to Enforcement Staff for issues identified during an Audit or a Spot Check
  - Recommendations should be supported by spreadsheet that includes:
    - Description of the issue
    - Assessment of the risk
    - Listing of mitigating activities, if any at that point
- While not "fix in the field," Compliance Staff may still verify what the registered entity does to mitigate the potential noncompliance

Example of FFT Spreadsheet

The Searchable FFT Informational Filing Spreadsheet is based on remediated issues that were submitted for informational purposes only. In the event of a conflict between information on the Searchable FFT spreadsheet and filed FFTs, the filed FFTs govern.

Informational Filing Date Regional Entity Registered entity NCR Issue Tracking # Standard / Requirement	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
	On April 11, 2012, XXX as a Transmission Owner, self-reported an issue with PRC-005-1a R2. During an internal review of XXX's Protection System maintenance and testing program, maintenance for a single transmission substation battery bank was identified as having a completion date which was past the interval-based due date by four days. Maintenance on the battery bank at issue should have been completed on September 30, 2011 and was actually completed on October 4, 2011.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the batteries were continuously monitored and an alarm would have alerted personnel in case of a voltage issue or an open battery bank. Additionally, the battery bank was only four days overdue for testing and maintenance. When tested, the batteries were found to be fully functional.	To mitigate this issue, XXX tested and maintained the battery bank that was out of interval, and trained the contractor and XXX personnel on the procedure and necessity for on-time maintenance.

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

http://www.nerc.com/page.php?cid=3|22
(CEI Resources)

Registered Entity's Responsibilities

- Compliance Staff's recommendations will not be made to the registered entity during an audit or spot check
- Whether through an Audit, a Spot Check, or a Self-Report, the registered entity should provide all of the information available on the possible noncompliance
  - Registered entity should avoid "lobbying" Compliance Staff for FFT treatment
  - Provide the best evidence to the Regional Entity and let that speak for itself

FFT Considerations

- In evaluating CIP noncompliance, avoid:
  - Stating that firewalls alone are effective mitigating controls for CIP-002 or -007 violations
  - Using the phrase "all of the requirements" or "all of the systems were protected" or "all other systems were compliant" and specify what was and was not in place
  - Making general statements about risk by focusing on specific compensating or mitigating measures for the Critical Asset or Critical Cyber Asset in scope
- Document input from your technical Subject Matter Experts
- Be aware of potential indications of process failures

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Examples of CIP FFTs and SNOPs

RELIABILITY | ACCOUNTABILITY




CIP-007-1 R4.1

- **Issue:**
  - During an energy management system (EMS) replacement, a legacy EMS system did not receive virus updates as described in the registered entity's anti-virus (AV) process in order to comply with CIP 007 R4.1.
  - As a result the registered entity's legacy EMS was potentially exposed to viruses and malware for a 37-day period while the new EMS system was being implemented (which utilized a different AV software and was receiving the required updates).

CIP-007-1 R4.1

- **Risk Considerations:** The legacy EMS was disconnected from the serial remote terminal unit (RTU) paths and its ability to affect the bulk electric system operations was minimal.
  - The legacy EMS was still within the electronic security perimeter (ESP) during the violation period
- **Mitigating Activities:** The region relied upon entity attestation that ESP access, monitoring and other security controls remained in place during the violation period.

Reasons for FFT treatment

- **Risk Determination:**
  - Minimal
- **Key Factors:**
  - The EMS was no longer connected to the field devices after the switchover was made.
  - Logs, ports/services and account access logs were reviewed during the violation period to ensure that malicious activity did not occur.

Risk Statement

- **Risk Considerations**
  - 37-day exposure
  - Core EMS platforms were involved
  - AV software was up-to-date on new EMS
  - Legacy EMS had limited command and control capability
  - Entity attestation verifying that underlying risk or residual risk was effectively assessed and mitigated

CIP-006 R1.1

- During a Compliance Spot Check, the Regional Entity discovered that the registered entity, as a Balancing Authority, Generator Owner, Generator Operator, Load Serving Entity, Transmission Operator, Transmission Owner, Transmission Service Provider and Interchange Authority, failed to identify six of its physical access control system (PACS) Cyber Assets and to afford them the protection required by CIP-006 R2.2.
- This condition existed from July 1, 2009 to August 22, 2011.

Determination of Risk

- **Risk Determination:**
  - Moderate
- **Key Factors:**
  - 782-day exposure
  - Physical access to CCAs could be compromised
  - If physical access is breached, protections afforded to the CCAs by other CIP requirements are nullified

Mitigation Considerations

- **Risk Considerations:**
  - The six systems were not afforded the overarching protection of the registered entity's cyber security policy nor the required oversight of a senior manager.
  - The personnel with access to these six systems were not screened with a personnel risk assessment program.
  - The six systems were not protected with the required technical and procedural controls to allow only authorized electronic access.
  - The six systems were not being monitored as required.

Mitigation Considerations

- **Key Factors Continued:**
  - The six systems did not necessarily receive all of the physical access controls and monitoring required.
  - Did these six systems have test procedures?
  - Were their ports and services managed?
  - Did they receive timely patches?
  - Were their passwords complex and changed frequently?
- At a minimum, all of the above should be considered in the mitigation plan.

CIP-007-1 R1

- **Issue:** A failure to use appropriate test procedures to ensure that new CAs and significant changes to CAs within the ESP do not adversely affect existing cyber security controls.
  - The entity periodically utilized an intermediate AV server to download AV signature and security patch updates for the CAs within the ESP but failed to test the server each time it was reintroduced into the ESP.

CIP-007-1 R1

- **Risk Considerations:** The entity did not consider the AV server to be a "new" CA each time it reconnected to the ESP, and therefore could not demonstrate that appropriate test procedures had been followed.
- **Mitigating Activities:** The entity ceased the practice of updating AV signatures using a temporary intermediate AV server, revised the EMS AV signature update process, and reviewed and confirmed all EMS cyber assets are properly identified and protected.

Reasons for NOP treatment

- **Risk determination:** Substantial
- **Key factors:**
  - The intermediate AV server utilized by the registered entity was configured as a hardened, single-purpose device, thus reducing the risk of compromise by malware or other exploits. – How was the system hardened? Who verified?
  - The registered entity tested anti-malware signatures and security patch updates in a development environment prior to introduction to the ESP.
  - The intermediate AV server was not connected simultaneously to the ESP and the registered entity corporate network. This does not assure that exposure is mitigated to ESP.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Identifying Operations and Planning FFTs and SNOPs

RELIABILITY | ACCOUNTABILITY




PRC-005-1 R2

- **Issue**: Failure to maintain and test transmission Protection System devices in accordance with the defined intervals in Protection System maintenance and testing program.
  - Failure to maintain and test 56 devices out of 861 total devices, or approximately 6.5%.
- **Risk Considerations**: The devices at issue were continuously monitored via a supervisory control and data acquisition system.
- **Mitigating Activities**: The entity completed inventory of each BPS device, developed a "catch-up" maintenance and testing plan and schedule, trained its technicians, and notified contractor personnel regarding revisions to the program.

Reasons for FFT treatment

- **Risk Determination**: Minimal
- **Key Factors**:
  - Less than 7% of devices were not tested, equating to a Lower VSL
  - The devices at issue were continuously monitored via a supervisory control and data acquisition system.
  - Size of the registered entity - annual peak of less than 600 MW in 2009

Risk Statement

- **Risk Considerations:**
  - Relays were being continuously monitored via supervisory control and data acquisition (SCADA) system
  - 56 devices out of 861 total devices involved, or approximately 6.5%
  - Size of registered entity's generation and transmission facilities

PRC-005-1 R1.1

- **Issue:** Documents of the registered entity's relay maintenance and testing program for the BPS did not show maintenance and testing intervals for its Current Transformer (CT) and Potential Transformer (PT) devices.
- **Risk Considerations**: The 70 total CTs and PTs at issue comprised fewer than 25% of the 408 applicable Protection System devices.
- **Mitigating Activities**: The registered entity revised its Protection System maintenance and testing program to include last testing date and next testing date for CT and PT devices.

Reasons for SNOP treatment

- **Risk Determination**: Moderate
- **Key Factors**:
  - Duration over several years
  - During the pendency of the violation, the registered entity verified the integrity of the CT and PT devices by performing testing periodically as per the registered entity's maintenance documents
  - The registered entity employs back-up relaying providing backup protection should the primary systems fail

Risk Statement

- **Risk Considerations:**
  - The registered entity employs back-up relaying providing backup protection should the primary systems fail.
  - The result of the CT and PT devices tested satisfactorily.
  - The duration spans over several years.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comparing Results and Discussing Common Challenges

RELIABILITY | ACCOUNTABILITY




Exercises

- Review facts, circumstances, and risks of the noncompliance
- Assess the risk of the noncompliance, including categorizing as minimal or moderate risk
  - Compose the risk statement
- Recommend appropriate disposition track
  - FFT or NOP

Discussion of Exercises

- Enough information to make a decision?
  - What information is most useful? Least useful?
  - What more do you need to know to come to a recommendation for disposition?
    - Are you able to provide that information to your Regional Entity?
- What information most affects the risk determination?
- What types of violations merit imposition of penalties?
- How confident were you in your recommendation of the disposition track?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Ongoing CEI Implementation and Development

RELIABILITY | ACCOUNTABILITY




CEI Ongoing Implementation

- Third Quarter 2012
  - September compliance enforcement authority (CEA) Staff workshop and training course
  - Begin random sampling of FFTs already filed with FERC
- Fourth Quarter 2012
  - Online webinar courses for CEA staff
  - All CEA compliance monitoring staff complete required training course
- 2013
  - Propose additional CEI improvements

Random Sampling

- Include results of sampling in 12-month status report to FERC (March 15, 2013)
- Begin sampling in September or October to have results by end of 2012
- Random selection of FFTs to survey using accepted sampling methodology
  - Ensures that reliability issues have been fixed as certified by the registered entity and that the issue has not recurred
  - Validates risk assessment and that penalty was not necessary
  - Monitors program and identify improvements rather than reopen FFTs or second-guess the Regional Entities
- FERC has announced a similar intent to survey a random sample of FFTs

CEI Pathway Forward

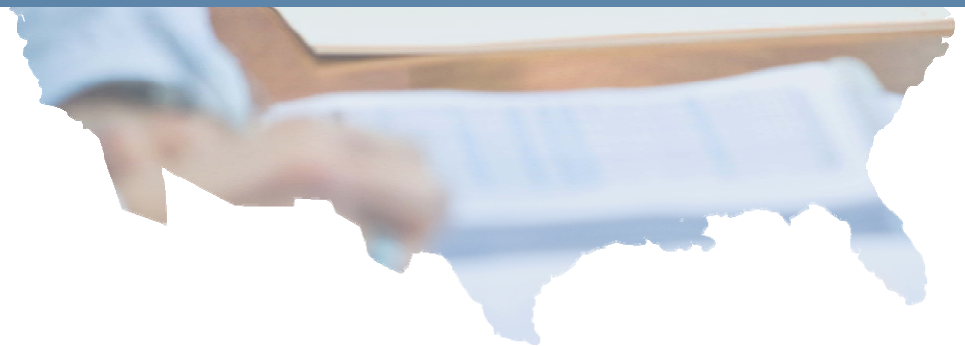
- NERC and the Regional Entities commenced development and planning
- The process will include:
  - Whitepaper
  - Pilot test of plan elements
  - Communication with Industry and FERC
  - Propose comprehensive approach in March 2013 CEI compliance filing

Conclusion

- FFT is a useful tool for handling minimal risk issues that do not require imposition of a penalty
  - Not just $0 penalty violations
- Gather as much information as possible about a noncompliance in order to allow for a robust risk assessment and easier decision on disposition track
- Collaborate with your Regional Entity on developing and packaging information to make processing of non-compliances more efficient

Questions

Questions and Answers



Contact Information

Ken Lotterhos
Associate General Counsel &
Director of Enforcement
(202) 400-3009
ken.lotterhos@nerc.net

Ed Kichline
Mgr. of Enforcement Processing
(202) 400-3025
ed.kichline@nerc.net

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 12th day of October, 2012.

/s/ Nina H. Jenkins-Johnston
Nina H. Jenkins-Johnston
Attorney for the North American Electric Reliability Corporation