

Agenda

Board of Trustees Compliance Committee Open Session

May 8, 2012 | 10:45 a.m.-Noon Eastern

Westin Arlington Gateway
801 North Glebe Road
Arlington, VA 22203
703-717-6200

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

1. **Minutes* — Approve**
 - a. February 8, 2012
2. **Compliance Enforcement Initiative (CEI)***
 - a. FERC Order — **Review**
 - b. Find, Fix, Track (FFT) Statistics to Date — **Information**
 - c. Ongoing Implementation of CEI — **Information**
3. **Compliance Operations***
 - a. Risk-Based Compliance Monitoring and Entity Assessments — **Information**
 - b. 2011 Annual Compliance Monitoring Enforcement Program Report — **Information**
 - c. CIP-005 Compliance Analysis Report — **Information**
4. **Regional Entity Items***
 - a. Reliability Standards Audit Worksheet (RSAW) Development — **Information**
5. **Quarterly Statistics***
 - a. Update on Quarterly Statistics to Fulfill the Committee's Mandate Obligations — **Information**

*Background materials included.

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Draft Minutes

Compliance Committee — Open Session

February 8, 2012 | 10:45 a.m.–Noon Mountain

Arizona Grand Resort
8000 S. Arizona Grand Parkway
Phoenix, AZ 85044
602-438-9000

Chair Bruce Scherr convened a duly noticed open meeting of the Compliance Committee of the North American Electric Reliability Corporation on February 8, 2012 at 10:45 a.m. local time, and a quorum was declared present. The agenda is attached as **Exhibit A**.

NERC Antitrust Compliance Guidelines

Chair Scherr directed the participants' attention to the NERC Antitrust Compliance Guidelines.

Minutes

The committee approved the November 2, 2011 meeting minutes (**Exhibit B**).

Compliance Committee Self-Assessment Results

Chair Scherr referred to the information contained within the Agenda Package, as well as to two slides presenting the most and least favorable results noting all of the results are yellow and green with two exceptions. Those exceptions based on the comments received with the responses raises the question if the Compliance Committee has in its charge the ability to complete those items.

The committee discussed reviewing the mandate to determine if changes are warranted.

Compliance Enforcement Initiative

Mr. Ken Lotterhos, associate general counsel and director of enforcement, conducted an update on the Compliance Enforcement Initiative (CEI) (**Exhibit C**). In overview, Mr. Lotterhos stated the initiative has been successful overall and has received solid support from the industry. Mr. Lotterhos provided that previously there had been one procedure for handling violations, completing a full Notice of Penalty (NOP). With the CEI filing, Compliance Enforcement gained two new reporting mechanisms - the spreadsheet NOP, as well as the Find, Fix, Track, and Report (FFT) spreadsheet. Mr. Lotterhos noted the FFT has the possibility of providing even greater benefits not only to the Regional Entities but also to the registered entities as well. The FFT process provides greater alignment of activity with the actual risk of the violation.

During the review of the *Number of FFTs filed at FERC by Regional Entity* chart, Board of Trustees Chair John Q. Anderson and Chair Scherr requested Mr. Lotterhos provide further detail on the reasoning for the numbers as presented noting WECC, by size of region, consistently has the most violations yet they are showing a low number on the chart. To assist in this answer, a representative from WECC responded stating there were multiple reasons for WECC's low numbers. First, several years ago, WECC submitted a significant number of violations to NERC for processing and an intervening FERC ruling sent them back to WECC, causing a large backlog. Second, WECC has a fairly small pool of candidates to select from and should there be a violation that is already in process bundled in a different form with other violations then WECC feels it is best to continue with one process than creating two. Third, a violation may be eligible for FFT but the entity has not yet completed mitigation; as a result, WECC prepares it as a Spreadsheet NOP. Finally, WECC is being selective in the candidates and is taking a conservative approach.

The committee discussed the need to ensure greater consistency and continuity across Regional Entities in the use of the new CEI tools. President and CEO Gerry Cauley committed that NERC Compliance Enforcement staff will complete a review of the practices across all Regional Entities, to ensure the process is working effectively and efficiently.

Ms. Rebecca Michael, associate general counsel, provide an update on the six-month CEI implementation report. She noted that staff has provided several opportunities for industry input, including an upcoming discussion at the Member Representatives Committee meeting, circulation of a survey that resulted in over 400 submittals by registered entities, and an opportunity for written comments due by February 23, 2012 to the email address ceicomments@nerc.net. Ms. Michael stated the report will address data and key trends, the guidelines employed today, potential benefits already realized and those hoped to be gained, implementation and transitional issues, and a request that the Commission act on NERC's September 30 filing.

Mr. Stanley Kopman, assistant vice president of compliance registration and enforcement for NPCC, reviewed his presentation (**Exhibit D**) which offered the regional perspective on the FFT initiative. Mr. Kopman stated that: (i) the FFT process has reduced violation processing time as well as NERC and Regional manpower requirements, and (ii) violations have been corrected, more expeditiously, through targeted and documented mitigating actions rather than use of the formal mitigation plan approval process. Together, this has resulted in enhanced focus on bulk power system reliability, not compliance administration. Further, FFT assessments have identified potential areas for Reliability Standard review and the possible elimination/revision of certain requirements. In conclusion, Mr. Kopman offered several ongoing recommendations:

- Consistent application of FFT Process, across Regional Entities, is a high priority for Regional Entities.

- Increased sharing of FFT Process applications (*e.g.*, mitigating actions, etc.) among Regional Entities will enhance consistency.
- Increased communication with the registered entities regarding examples of potential FFTs and appropriate mitigating actions would be beneficial.
- NERC IT needs to set up metrics for CRATS reporting so FFT reporting is correctly captured with regard to submitted mitigation activities.
- Closure of FFT candidates needs to be documented definitively; regulatory closure would be beneficial.
- Further expansion of the FFT process will depend on training of auditors and industry education in Phase 2, to ensure consistent expectations and application of the process.

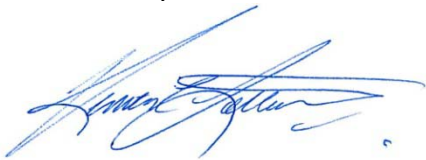
Trustee Ken Peterson noted that feedback from compliance to standards is critical and inquired of Mr. Kopman what mechanisms are in place or would like to see in place to ensure this communication is occurring. Mr. Kopman responded that one mechanism is the Regional Entities working more closely with the Regional Standards Committees and a second mechanism is to assess the results of the FFT determinations and look at how the standards are written and then ensure that analysis is distributed to the appropriate standards body.

Quarterly Statistics

Chair Scherr referenced the materials provided in the Agenda package. **(Exhibit E)**

There being no further business, Chair Scherr adjourned the meeting at 12:04 p.m. Mountain.

Submitted by,



Ken Lotterhos
Associate General Counsel and Director of Enforcement

Compliance Enforcement Initiative

Action

Discussion

Summary

NERC continues to process violations through the streamlined Spreadsheet Notice of Penalty (SNOP) and the Find, Fix, Track and Report (FFT) informational filing. Since the initial Compliance Enforcement Initiative (CEI) filing on September 30, 2011, NERC will have made eight SNOP filings and eight FFT filings with the Federal Energy Regulatory Commission (FERC) through the end of April 2012. The Commission has issued orders of no further review on the SNOP and NOP filings submitted through the end of February.¹

On March 15, FERC issued an order on the CEI filing. The Order provided:

- All six FFT filings, through February 2012, were accepted;
- Violations are final 60 days after submittal unless there is cause to open for review;
- Prospectively, violations must be of minimal risk to the bulk power system; this condition may be revisited after the one-year status report filing;
- Registered Entities must certify that violations are remediated;
- Registered Entities must be identified in filings, except for cases of critical infrastructure protection violations;
- FERC will conduct random surveys each year to gauge program performance; and
- NERC, Regional Entities and interested entities may propose mechanisms to identify and remove unnecessary or redundant requirements from Commission-approved reliability standards.

The March 15 Order requires NERC to make a compliance filing in addition to its six-month status report; both due on May 14, 2012. NERC's compliance filing will explain how NERC and the Regional Entities will evaluate a registered entity's compliance history when deciding if FFT treatment is warranted and will provide additional information on how NERC will continue to implement the FFT program. Extension of the ability to identify and process FFTs to compliance monitoring personnel will be a key part of the compliance filing and NERC's efforts over the next several months.

As part of its six-month status report to the Commission, NERC will describe the experience gained and the results from implementation of the CEI to date. Specifically, the six-month report will address and provide context for the CEI processing statistics, discuss the benefits obtained from the program from a broad perspective (NERC, Regional Entity and industry), how NERC is addressing them. In preparation for this filing, NERC will be working with the Regional Entities to ensure their input is incorporated into the filing.

¹ Action on the March 30, 2012 filing is expected by April 30, 2012.

To date, the CEI has received significant support from the Regional Entities and the industry. NERC anticipates the FFT process will continue to enable better alignment and substantially greater resources and attention to be devoted to matters that pose a more serious risk to the reliability of the bulk power system. NERC will be working collaboratively with the Regional Entities' compliance and enforcement staffs as well as the industry throughout 2012 to continue to implement and improve the CEI.

Risk-Based Compliance Monitoring and Entity Assessments

Action

Information

Background

This update was provided at the Member Representatives Committee (MRC) Informational Meeting held on May 1, 2012. It will also be provided as background material for the MRC Chair's discussion at the MRC meeting held on May 8, 2012.

The purpose of this update is to provide a comprehensive overview for the Risk-Based Compliance Monitoring Initiative. The slide presentation addresses NERC's purpose for the initiative, what success would look like, and the NERC projects that support the initiative.

The initiative, which is being implemented through the projects listed below, integrates the concept of risk, to a greater degree, into ERO compliance and enforcement. Identification of risk allows for resources to be focused on those issues that pose the greatest risk to the reliability of the bulk power system (BPS). The initiative also provides for a paradigm shift from backward-looking compliance monitoring to an empowerment for entities to be forward-looking and successful in their compliance activities. This initiative integrates the evaluation of risk throughout the process — at the program level, the entity level and in the enforcement processing level, as follows:

Program Level

- Annual Implementation Plan
- Actively Monitored List

Entity Level

- Entity Assessment — The assessment (or evaluation) will, among other objectives, determine scope and frequency of compliance monitoring for each entity.
- Compliance Monitoring — Integration of verification of internal controls into the compliance monitoring to determine the due diligence a CEA is to use (the amount of evidence to review) to obtain reasonable assurance the entity is not non-compliant.

Enforcement Processing Level

- Resolution of non-compliance based on risk (CEI)
 - Find, Fix and Track — Lower Risk Possible Violations
 - Notice of Penalty

Summary

This initiative is designed to:

- Allow for focus of resources on reliability issues.
- Empower registered entities to be forward-looking and successful in their compliance activities.

The major change elements of this initiative are assessing the frequency and scope of an entity's compliance monitoring based on the individual entity's potential impact on the reliability of the BPS, the integration of formal audit principles into compliance monitoring including assessing internal controls, and the implementation of CEI Phase II, where discretion is applied in the field.

Risk-Based Reliability Compliance Monitoring

April 20, 2012

As the Electric Reliability Organization (ERO) continues to evolve, greater emphasis has been placed on incorporating risk-based concepts in all endeavors to more efficiently utilize resources and focus on the significant risks of the electrical sector. From the ERO Enterprise Strategic Plan 2012-2015 approved in February of 2012, the following vision is detailed:

“To be the trusted leadership that ensures and continuously improves the reliability of the North American bulk power system (BPS) by implementing relevant standards; promoting effective collaboration, cooperation, and communication around important risks to reliability; and utilizing expertise from the industry to produce outcomes that improve reliability.”

Within the strategic plan, the four Pillars for Success clearly articulate the critical components that will be emphasized to achieve this vision:

- **Reliability** – to address events and identifiable risks, thereby improving the reliability of the BPS.
- **Assurance** – to provide assurance to the public, industry, and government for the reliable performance of the BPS.
- **Learning** – to promote learning and continuous improvement of operations and adapt to lessons learned for improvement of BPS reliability.
- **Risk-Based Approach** – to focus attention, resources and actions on issues most important to BPS reliability.

The purpose of this paper is to provide a comprehensive overview of the Risk-Based Compliance Monitoring Initiative and its components; the initiative’s background; the necessity of making compliance a tool that supports reliability; an articulation of success; and the criticality of greater consideration of internal controls; as well as to identify potential Rules of Procedure (ROP) changes. The NERC corporate goals for 2012 firmly direct these efforts, specifically within Goal No. 1 for Standards and Compliance, performance objective c: *Promote a culture of compliance with mandatory reliability standards across the industry*. Successful implementation of the performance objective will be, in part, determined by the following measures:

- 11 – Educate industry on effective compliance programs and effective reliability risk controls.
- 12 – Develop risk-based compliance monitoring approaches to maximize reliability benefits and improve efficiencies, and to encourage effective internal controls at registered entities.

Additionally, the ERO will support the industry by identifying procedures, practices and controls to address reliability risks resulting from noncompliance.

Overview

In late 2010 and early 2011, industry and NERC staff began discussions of risk-based compliance monitoring with a goal of refining compliance and enforcement efforts to support reliability efforts. Initial efforts between industry and NERC staff included greater analysis to support development of the Annual Implementation Plan and Actively Monitored List (AML); discussion of refined compliance monitoring concepts to include appropriately scoped audits and spot checks; a white paper developed by Tom Burgess; and the NERC Compliance and Certification Committee (CCC) Work Group's effort to refine issues and develop options for future direction.

Ultimately success for both the ERO and the industry will be based on a clear set of concepts that include an emphasis on reliability and less compliance bureaucracy; compliance programs designed to support reliability on a forward-looking basis with greater reliance on internal controls; an industry that monitors, finds, fixes, tracks, and reports (FFT) issues; and refocused resources to allow us to address high-risk reliability issues. The Risk-Based Compliance Monitoring Initiative will manifest these concepts in:

- Registered entities that are empowered to be in control of monitoring their own compliance activities and have successful compliance programs.
- ERO and industry resources being focused on reliability.
- The successful implementation of a risk-based approach to compliance monitoring.

There must be greater emphasis on reliability and less on compliance and enforcement bureaucracy. While the requirements are enforceable, shifting to greater consideration of the intent and purpose of the standard will provide greater opportunity for industry collaboration and information sharing to meet reliability obligations.

The ERO compliance monitoring program and registered entities' compliance programs should be designed to support reliability on a forward-looking basis with greater consideration and reliance on internal controls. The current construct is focused on the rearward-looking process of reviewing potentially significant amounts of evidence over the entire audit period. Further, all violations, regardless of the risk created to the reliability of the BPS or when the violation occurred, must be processed. This rearward-looking approach to compliance monitoring provides little to no confidence that the entities have the ability to make judgments about their future state of reliability.

An emphasis on internal controls and how an entity manages its own compliance programs is forward-looking. Internal controls are proactive and, coupled with a solid internal compliance program, will

demonstrate an entity's commitment to manage compliance with a focus on reliability until the next compliance monitoring effort. The industry has already demonstrated a commitment to compliance as evidenced by the high numbers of self-identified possible violations (PVs); 69 percent in 2011 and 68 percent over the entire enforceable period (2007-present). Self-identified violations include four of the eight compliance monitoring program discovery methods: self reports, self certifications, data submittals and exception reporting. This is a significant factor in the reasoning for the Compliance Enforcement Initiative (CEI) and the FFT mechanism. The industry has demonstrated that it does indeed monitor, FFT compliance issues and PVs.

With this proactive and responsible compliance mentality, both the ERO and industry can focus more resources on high-risk reliability issues and less on compliance. Registered entities will be able to deploy and utilize resources to improve reliability as opposed to managing compliance risk and the volumes of data required to demonstrate compliance on a rearward-looking basis.

Consideration of internal controls and internal compliance programs are basic auditing concepts and principles designed to be forward-looking. These concepts are articulated in detail in the "Yellow Book" or Government Auditing Standards, which were most recently revised in December 2011.¹ Other auditing organizations and references include the Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework^{2,3} and the Public Company Accounting Oversight Board (PCAOB)⁴

Key components of auditing include rigorous planning and preparation, appropriate field work, and reporting to communicate the audit team's results. Planning and preparation must include an assessment of the organization to be audited and a consideration of the internal controls. The finding of the audit must be based on the auditor's professional judgment in obtaining reasonable assurance of compliance. Based on the level of the performed audit, an auditor may not have sufficient knowledge to determine that an entity is compliant; only that there was not a finding of non-compliance. Finally, reporting must communicate the results for the intended purpose of the program.

Reasonable Assurance as discussed in the International Federation of Accountants (IFAC) / The International Auditing and Assurance Standards Board (IAASB)'s International Standards on Auditing #200⁵, Introduction is:

"Reasonable assurance is a high level of assurance. It is obtained when the auditor has obtained sufficient appropriate audit evidence to reduce audit risk . . . to an acceptably low level. However, reasonable assurance is not an absolute level of assurance, because there are inherent limitations of an audit which result in most of the audit evidence on

¹ Available at: <http://www.gao.gov/products/GAO-12-331G>, April 2012.

² <http://www.coso.org/>

³ Members include American Accounting Association, American Institute of CPAs, Financial Executives International, The Association for Accountants and Financial Professionals in Business, and the Institute of Internal Auditors

⁴ <http://pcaobus.org/Pages/default.aspx>

⁵ Available at: <http://www.ifac.org/sites/default/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf>, April 2012.

which the auditor draws conclusions and bases the auditor's opinion being persuasive rather than conclusive."

Professional Judgment from GAGAS Section 6.03 is detailed as:

*"Objectives for performance audits range from narrow to broad and involve varying types and quality of evidence. In some engagements, sufficient, appropriate evidence is available, but in others, information may have limitations. **Professional judgment** assists auditors in determining the audit scope and methodology needed to address the audit objectives, and in evaluating whether sufficient, appropriate evidence has been obtained to address the audit objectives."* [emphasis added]

Components of the Risk-Based Compliance Monitoring Initiative

As NERC moves towards greater consideration and utilization of risk-based concepts and methods in the Compliance Monitoring and Enforcement Program (CMEP)⁶, the following levels have been identified for focus: the program level, specifically the Annual Implementation Plan and AML; the registered entity level, where development of the entity assessment is critical; and the compliance issue or violation level.

The Program Level

At the program level the Risk-Based Compliance Monitoring Initiative focuses in two areas: the development of the AML and communication of compliance assessment approaches, specifically through the Reliability Standard Audit Worksheets (RSAWs).

The AML

The AML will identify the highest priority standards for compliance monitoring. These standards will establish the baseline or starting point for the Regional Entity (RE) in developing an appropriate scope of compliance monitoring for an individual registered entity, based upon the results of the Entity Impact Evaluation (see discussion on appropriately scoping compliance monitoring below). The highest priority Reliability Standards and associated Requirements populating this list are determined annually through a review of the following:

- ERO High-Risk Priorities
- FERC Orders and Guidance
- Compliance History and Culture
- Input from NERC Staff including Compliance Operations, Critical Infrastructure Protection, Enforcement, Events Analysis and Investigations, Legal, Reliability Assessments and Performance Analysis, and Standards

⁶ Available at: http://www.nerc.com/files/Appendix4C_Uniform_CMEP_20110101.pdf

- Future Considerations

Communication of Compliance Assessment Approaches through the RSAWs

To clearly communicate compliance assessment approaches, NERC has begun to update the RSAWs by integrating the standard drafting team's intent, obtaining broader industry input and resolving compliance monitoring approaches. The objective of obtaining this input is to reduce any gap between the drafting team's intent for the standard and compliance expectations. Compliance and enforcement will continue to own the RSAWs to ensure Compliance Enforcement Authorities (CEAs) appropriately and consistently monitor compliance; however it is expected that this integration effort will, as RSAWs are modified, prevent spikes in the number of violations when standards become enforceable and prevent unnecessary violations for existing standards. Further, this effort will, to the extent possible, consolidate compliance guidance documents into one location, where CEAs and registered entities can easily access all relevant information. It is anticipated that the improved understanding that comes along with the updated RSAWs will reduce the number of requests for standard interpretations and compliance application notices (CANs).

NERC is also beginning to introduce formal auditing principles⁷, including the assessment of internal controls, into the RSAWs.⁸ As discussed above, this widely accepted auditing practice provides auditors an opportunity to assess whether a registered entity has control over its own compliance activities and the ability to use that assessment to determine the level of due diligence that will be required during the audit. Using this method, the auditor has the ability to monitor the entity's internal controls, which are not subject to compliance, and use the entity's evidence of compliance activities to verify the effectiveness of the internal controls. The updated RSAWs introduce these concepts with a discussion of the purpose for assessing internal controls during an audit and a reminder for an entity to provide an auditor or CEA with its internal controls (see discussion on incorporating internal controls into compliance monitoring below).

The Entity Level

At the entity level the Risk-Based Compliance Monitoring Initiative focuses on two areas: the implementation of Entity Impact Evaluations, and inclusion of auditing principles, specifically internal controls, into compliance monitoring.

Entity Impact Evaluations

An open and transparent Entity Impact Evaluation will provide a consistent method for Regional Entities (Res) to determine appropriately scoped, or customized, compliance monitoring for each registered entity. The Entity Impact Evaluation will be a non-public evaluation that, in the successful

⁷ Utilized in Generally Accepted Government Auditing Standards (GAGAS) and outlined in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) model; members of COSO include the American Accounting Association, American Institute of CPAs, Financial Executives International, The Association for Accountants and Financial Professionals in Business, and the Institute of Internal Auditors.

⁸ The location of internal control information will be determined based on industry preference, but may be located either in each individual RSAW or in an overarching RSAW document that may also contain other information pertaining to multiple RSAWs.

implementation of the Risk-Based Compliance Monitoring Initiative, will be initially performed by the registered entity and completed in collaboration with the RE.

The results of an entity's Entity Impact Evaluation will determine the frequency of future compliance monitoring, the methods of compliance monitoring, and the number of standards that will be included in a registered entity's appropriately scoped compliance monitoring. The Entity Impact Evaluation will consist of four elements:

- The entity's internal controls, Internal Compliance Program and regional considerations;
- The entity's technical factual information (such as the number of transmission miles, etc);
- The entity's performance in each of its registered functions; and
- The entity's compliance history story.

All entities will have the ability, and are encouraged, to influence the amount of compliance monitoring that it will receive by managing their above four elements. An entity may not be able to change its technical facts; however an entity may have the ability to alter its performance metrics, the story behind its compliance history or its internal controls and internal compliance program. In the vision of success, the majority, if not all, entities will manage the four elements of their Entity Impact Evaluation and will qualify for less compliance monitoring.

There criteria to be considered in a review of the entity's internal controls and internal compliance program are interwoven. The internal compliance program elements are outlined in a series of FERC orders⁹ and include the original 13 questions as well as the four hallmarks. The COSO model¹⁰ is used as a guideline for evaluating the internal controls; it provides a framework consisting of five elements. Three of the five elements are considered in the Entity Impact Evaluation – the Control Environment, the Risk Assessment, and Information and Communication. The remaining two elements, Internal Control Activities and Monitoring Internal Controls, are verified during compliance monitoring. Internal controls are not subject to compliance but will affect the level of due diligence an auditor will conduct for evidence that is subject to compliance.

For example, an entity that may have more impact to the BPS from a technical perspective may have demonstrated good performance, a positive story behind its compliance history and strong internal

⁹ Policy Statement on Enforcement (13 questions) Docket No. PL06-1-000, 113 FERC ¶ 61,068 (October 20, 2005); Revised Policy Statement on Enforcement Docket No. PL08-3-000, 123 FERC ¶ 61,156 (May 18, 2008); Policy Statement on Compliance (4 Hallmarks) Docket No. PL09-1-000, 125 FERC ¶ 61,058 (October 16, 2008); Policy Statement on Penalty Guidelines Docket No. PL10-4-000, 130 FERC ¶ 61,220 (March 18, 2010); suspended on April 15, 2010; Revised Policy Statement on Penalty Guidelines (Additional criteria during a FERC 1.b investigation) Docket No. PL10-4-000, 132 FERC ¶ 61,216 (September 17, 2010)

¹⁰ This procedure is based on the Internal Control – Integrated Framework (1992) COSO model and subsequent Guidance on Monitoring Internal Control Systems (2009), which emphasizes the monitoring element of the 1992 model.

controls. The positive elements of the Entity Impact Evaluation may offset the potential high impact to the grid, qualifying the entity for less compliance monitoring.

In another example, a registered entity may have effective internal controls and an effective internal compliance program, non-impactful technical factual information, a good compliance history story and perform well in all its registered functions, except one. That entity may qualify for less compliance monitoring with some spot checking in the area with a need for improvement.

There are currently activities for the development of the Entity Impact Evaluation template underway — one is a broad-based working group under the CCC, and the second is a series of focus groups that will provide feedback to the CCC working group. The focus groups will provide input regarding performance metrics that would provide a fair and accurate representation of a specific function within one entity. These two efforts, along with input from the REs, will be combined into one draft and will be posted for industry comment in early summer 2012. It is a NERC goal to have the completed template posted on the NERC website for use by the end of 2012. The REs may begin using the Entity Impact Evaluation template in 2013; however it is anticipated that the Entity Impact Evaluation will be implemented slowly over the next few years.

Inclusion of Auditing Principles, Specifically Internal Controls, into Compliance Monitoring

The inclusion of internal controls into compliance monitoring represents a paradigm shift from rearward-looking monitoring of compliance over the entire audit period to forward-looking monitoring of an entity's internal controls, which will determine the amount of due diligence required for an auditor to assess compliance — i.e., the amount of evidence that is necessary to review.

The amount of due diligence required will be based on whether the entity's internal controls are effective. In this context, being effective means that the registered entity's internal controls are finding any human drift in performance or any non-compliance at potential failure points in their compliance activities; the entity is fixing the drift or non-compliance; the entity is tracking the mitigation of the drift or non-compliance as well as any future occurrences; and if the entity determines there has been a PV, it is reporting the PV to the applicable RE. Under this method, the entity may assess and remediate issues using the FFT mechanism so lesser or minimal-risk issues do not detract from moderate and high-risk issues.

Where an entity has effective internal controls, a CEA will pull a reduced sampling from recent activity to verify that the entity's internal controls are working. If the sampling demonstrates that the entity's internal controls are working, the CEA will determine there is reasonable assurance of compliance. This provides a forward-looking approach to compliance monitoring, as effective internal controls is an indication of future compliance performance. If the sampling demonstrates that the entity's internal controls are not working, the CEA will be required to conduct more due diligence to determine if the entity has any non-compliance. In either case the CEA will sample recent activity and will not seek to

verify whether there has been any historical non-compliance over the entire audit period, unless there are specific concerns or reasons to do so. The results of this verification of the entity's internal controls will be used to update the Entity Impact Evaluation.

COM-002, specifically three-part communication, may be used as an example of internal controls. For this example, the compliance activity is the act of conducting the three-part communication. The internal controls for the entity consists of its supervisor pulling and reviewing 30 minutes of recorded tapes each week, plus listening to several live conversations per week. This allows the supervisor to identify any human drift away from compliance with reliability standards before a PV occurs.

Another entity separates their internal controls for this same standard into two categories: preventative controls and detective controls. Its preventive controls are comprised of processes, procedures, tools and signage, including its: Accident Prevention Manual; Annual Directive Training (Energy Control Center (ECC) Operators); Reliability Coordinator (RC) Directive Format (ECC Document); Guideline for Proper Communications (ECC Procedure); Safety Stand Down Presentations (Fossil Plants); Module in the "Conduct of Shift Operations & Maintenance Training" (Fossil Plants); Fossil Plant training "3-Way Communication Human Performance Tool"; and three-way communication signs in control rooms of fossil power plants. This entity's detective controls include random monitoring of calls by ECC Supervisors and supervisors on the floor in the ECC observations.

In summary, implementing auditing principles, including Internal Controls, offers many benefits:

- Internal controls are not enforceable, so provide an opportunity for entities to demonstrate forward-looking capabilities without being subject to compliance.
- Internal controls provide the maximum flexibility for entities to demonstrate their control over compliance activities.
- Internal controls provide an opportunity for entities to FFT any non-compliance or identify and correct human drift prior to having a PV.
- Provides an opportunity for additional auditor training to assess internal controls and emphasize as a means for greater reliability benefit.
- Provides less emphasis on auditors reviewing mountains of evidence.
- Provides greater emphasis on forward-looking compliance monitoring.

The Enforcement Processing Risk Level

The FFT Violation Processing Methodology

In 2011, the ERO began processing lesser- and minimal-risk violations through the FFT process. The process was designed to expedite processing for lesser or minimal risk PVs by making a rapid determination of the risk, verifying that the non-compliance had been mitigated, and then resolving the

issue without the need for extensive evidence and paperwork. The process has been met with great success and, with some stipulations, approval from FERC in the March 15, 2012 order. Front-end work to determine whether a PV qualifies for FFT treatment will diminish as the process matures, auditors are trained, and FFT determinations are made in the field.

How Do We Get There?

It bears repeating that success for both the ERO and the industry ultimately will be based on a clear set of concepts that include an emphasis on reliability with less compliance bureaucracy; compliance programs designed to support reliability on a forward-looking basis with greater reliance on internal controls; an industry that monitors, FFTs issues; and refocused resources to allow industry and the ERO to address high-risk reliability issues. The Risk-Based Compliance Monitoring Initiative will manifest these concepts in:

- Registered entities that are empowered to be in control of monitoring their own compliance activities and that have successful compliance activities.
- ERO and industry resources being focused on reliability.
- The successful implementation of a risk-based approach to compliance monitoring.

Getting there will require a paradigm change in the ERO and industry's approach to compliance monitoring and enforcement. "Consistency" will take on a new meaning; rather than all registered entities being monitored for compliance in the same manner, consistency will mean that registered entities' impact to the bulk power system will be evaluated in the same manner. This evaluation will result in each registered entity having an appropriately scoped compliance monitoring program that has been customized with the frequency, methods, scope (number of standards) and depth (level of due diligence) of compliance monitoring adjusted in totality or in specific functional areas.

The ERO's path to this end goal involves several processes, as defined below.

The Program Risk Level – the AML and RSAWs

The AML will continue to exist in order to provide a basic framework of standards as a starting point for a REs determination for appropriately scoped compliance monitoring for a specific entity. RSAWs will evolve as they become aligned with the standards drafting teams' intentions and are communicated to FERC, or the appropriate regulatory body, during the standard's regulatory approval. This evolution will occur as the RSAWs are developed for new or changing standards, or as the RSAWs are revised for currently existing standards.

The AMLs will be created each year based on risk profiling, and the RSAWs will begin to be aligned with the standard drafting teams' intent for compliance monitoring.

The First Entity Risk Level – Entity Impact Evaluation

Entities will have the ability to influence the amount of compliance monitoring that they will receive based on the factors considered in the Entity Impact Evaluation. In a successful implementation of the Risk-based Compliance Monitoring Initiative, entities would conduct their own Entity Impact Evaluation using the four criteria:

- The entity's internal controls, Internal Compliance Program and regional considerations;
- The entity's technical factual information (such as the number of transmission miles, etc);
- The entity's performance in each of its registered functions; and
- The entity's compliance history story.

Further, a registered entity will provide their self-conducted Entity Impact Evaluation with their RE and collaborate on the evaluation. In the vision of success, the majority, if not all entities will manage their Entity Impact Evaluation and will qualify for less compliance monitoring.

Thus, another step to a successful implementation of the Risk-Based Compliance Monitoring Initiative is for registered entities to conduct their own Entity Impact Evaluations, assume control of monitoring their compliance activities using internal controls and work with their RE.

The Second Entity Risk Level – Internal Controls in Compliance Monitoring

The second level of risk assessment at the entity level occurs during the compliance monitoring, with the implementation of generally accepted auditing principles. Two aspects of internal controls, Internal Control Activities and Monitoring Internal Controls, are verified during compliance monitoring and will determine the level of due diligence a CEA will be required to perform to obtain reasonable assurance that there isn't any non-compliance, as discussed above. This verification of the entity's internal controls will be included in the next update of the Entity Impact Evaluation.

Thus, another step toward successful implementation of the Risk-Based Compliance Monitoring Initiative is for registered entities to create or identify internal controls that may be evaluated, but are not subject to compliance, during compliance monitoring activities. In the event that a registered entity does not have internal controls, traditional or status quo compliance monitoring will be conducted unless the CEA determines that increased due diligence is required.

The Enforcement Processing Risk Level – the Find, Fix and Track (FFT) Violation Processing Methodology

As discussed above, this processing method has been met with great success and, with some stipulations, approval from FERC in the March 15, 2012 order. However, there are still advancements for efficiency that can and should be made to complete the successful implementation of risk-based compliance monitoring.

These advancements include:

- Identifying criteria for a lesser or minimal risk PV (FERC restricted FFT candidates to lesser or minimal-risk PVs for the foreseeable future);
- Train auditors to readily identify FFT violations in the field in order to gain efficiencies on the front end of the processing cycle;
- Provide auditors with the authority to determine whether a non-compliance or PV qualifies for FFT processing;
- Obtain consistency in application across RE enforcement and auditing staff;;
- Pursue regulatory approval for the REs to track the FFT PVs without submission to the applicable regulatory body; and
- Obtain regulatory approval for moderate-risk PVs to be considered in the FFT process.

Changes to the ROP

While the ERO has the authority to implement the Risk-Based Compliance Monitoring Initiative under the current ROP, there are two sections that may require removal or modification to provide flexibility for establishing an appropriately scoped compliance monitoring program. The two sections in the Compliance Monitoring and Enforcement Program (CMEP) are:

- Section 3.1.4.2, Period Covered; and
- Section 11 Compliance Audits of BPS Owners, Operators, and Users.

Section 3.1.4.2 addresses the CEA requiring evidence of compliance over the entire audit period. It provides, in pertinent part:

- Section 3.1.4.2, Period Covered
 "...However, if a Reliability Standard specifies a document retention period that does not cover the entire period described above, the registered entity will not be found in non-compliance solely on the basis of the lack of specific information that has rightfully not been retained based on the retention period specified in the Reliability Standard. However, in such cases, the Compliance Enforcement Authority will require the registered entity to demonstrate compliance through other means."

Section 11 addresses the minimum frequency of audits for Balancing Authorities (BA), RCs or Transmission Operators (TOP). It provides, in pertinent part:

- Section 11 Compliance Audits of BPS Owners, Operators and Users
 - ...
 - 11.1 For an entity registered as a Balancing Authority, RC, or TOP, the Compliance Audit will be performed at least once every three years.

Therefore, another step to the successful implementation of the Risk-Based Compliance Monitoring Initiative is for the ERO to modify the ROP CMEP to allow flexibility for establishing an appropriately scoped compliance monitoring program that is unique to each entity and to focus on current compliance activity.

Lastly, the ERO and industry must continuously evaluate if the program is achieving its goal to increase the focus on reliability and course correct as necessary.

Summary

This shift in the approach to compliance monitoring has two main purposes:

- To empower registered entities to be in control of monitoring their own compliance activities and to enable entities to have successful compliance activities.
- Focus ERO and industry resources on reliability.

The use of risk-based compliance monitoring with an emphasis on internal controls can provide a model for assessing compliance that:

- Is forward-looking:
 - Rather than gathering evidence for the entire audit period (backward-looking), evidence of recent activities will be used to verify effectiveness of internal controls (forward-looking).
- Appropriately scopes compliance monitoring for each entity:
 - Frequency of compliance monitoring.
 - Method of compliance monitoring.
 - Number of standards or requirements or both included in compliance monitoring.
 - Level of due diligence required during compliance monitoring activities.
- Removes issues surrounding data retention beyond what is required by the standard:
 - Although entities are encouraged to keep data, this approach removes compliance concerns for entities regarding data retention beyond what is required by the standard.

- Provides incentive for industry to take control of compliance monitoring and compliance activities as compliance monitoring is focused, as appropriate, on internal controls that are not subject to compliance:
 - Effective internal controls will detect human drift before non-compliance occurs, providing the entity an opportunity for course correction.
 - Shift from a number consideration or discussion such as whether zero tolerance is appropriate for each standard or requirement. This is not the correct consideration as the number of non-compliance actions frequently doesn't equate to risk.
 - In the event of a PV, the entity may, for lesser or minimal-risk violations, use the FFT (find, fix, and track) processing method after reporting the non-compliance to its registered entity.
- Will ensure compliance as a necessary component of reliability. The emphasis is for the entity to self-monitor and self-report any non-compliance; however, CEAs will be looking to verify that an entity's internal controls are effective. If an auditor discovers a non-compliance that wasn't self-reported, additional due diligence will be required to determine a reasonable assurance of compliance.
- Focuses on issues that provide potential for the greatest impact to the reliability of the BPS.
- Encourages focus on reliability and associated risks.

Not all registered entities are the same; each is unique in its strengths and weaknesses, and each represents different levels of potential impact to the BPS. Similarly, different acts of non-compliance (whether a PV or a Violation) represent different levels of risk to the reliability of the BPS. The ERO is challenged to evaluate the potential impacts to the reliability to the BPS with the same criteria, but address each according to the associated risk.

The Risk-Based Compliance Monitoring Initiative provides the framework for such customization and focus. Its successful implementation will enable entities to monitor their own compliance activities and be successful in those endeavors; it supports the more efficient FFT method of reporting lesser or minimal-risk violations and, in turn, will allow resources to address issues that create a higher risk to the reliability of the BPS.

2011 Annual Compliance Monitoring Enforcement Program Report

Action

Approve 2011 Annual Compliance Monitoring Enforcement Program Report (CMEP) Report.

Summary

The 2011 CMEP Annual Report provides details, analysis, lessons learned, and forward looking activities regarding the Electric Reliability Organization's (ERO) implementation of the CMEP in 2011. The information needed to complete the report was collected from the eight Regional Entities (RE) and North American Electric Reliability Corporation (NERC) staff. Specific areas where information was received from NERC staff include the Compliance Operations department's Audit Assurance and Oversight (AAO), Compliance Interface and Outreach, and Organization Registration and Certification groups, the Reliability Risk Management department's Event Analysis and Investigation Teams (EA) and Human Performance groups, the Standards Development group, the Compliance Enforcement department, the Critical Infrastructure department, and the Legal and Regulatory department. In early 2012, the Regional Entities provided insights into the implementation of the CMEP from their perspective by reporting information to NERC about their CMEP programs via a survey. Additionally, the Regional Entities proposed a number of improvements for future iterations of the CMEP based upon their first hand experience while implementing the CMEP in 2011.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Compliance Monitoring and Enforcement Program

2011 Annual Report

April 1, 2012

RELIABILITY | ACCOUNTABILITY



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

Table of Contents

Table of Contents.....	ii
Executive Summary.....	1
NERC Staff CMEP Activities	1
Regional Entities CMEP Activities	2
Significant 2011 Projects.....	3
Acknowledgement	5
Introduction	6
Background	7
CMEP Process.....	7
NERC Staff CMEP Activities	9
Compliance Operations Department.....	9
Audit Assurance and Oversight Group	9
Risk-Based Approach	10
Seminars and Communications	11
Auditor Training Activities	11
Reliability Standard Audit Worksheets	12
Key Reliability Standards Spot Check.....	12
Regional Entity Program Audits - Agreed Upon Procedures (AUP) Spot Check	13
Compliance Interface and Outreach Group.....	13
Compliance Application Notices	14
Organization Registration and Certification Group	17
Multi-Regional Registered Entity (MRRE)	18
Organization Certification	19
GO/TO Directive.....	19

Public Notices.....	20
Compliance Analysis Reports.....	21
EOP-005 – System Restoration Plans.....	21
TOP-002 – Facility Ratings Methodology.....	21
VAR-002 - Generator Operation for Maintaining Network Voltage Schedules.....	21
NERC Organization Certifications	21
NERC Compliance Registry and Registration Appeals	22
Reliability Risk Management Department.....	22
Human Performance.....	24
Standards and Training Department	24
Standards Development	24
Critical Infrastructure Protection Standards.....	26
Enforcement Department.....	27
Enforcement Processing	36
Regional Entities CMEP Activities	38
Compliance Monitoring	38
Compliance Outreach	39
Compliance Enforcement	40
Program Effectiveness	41
Events Analysis and Compliance Review	42
Regional Entity Metrics	43
Projections for the Future.....	43
Significant 2011 Projects.....	46
Defining the Bulk Electric System	46
Find, Fix, and Track	47

FFT Filing	47
FFT Implementation	48
Registered Entity Assessment	50
Human Performance	51
CAN Revision Process	51
Rated System Path Methodology – MOD-029	52
Future of the CMEP	54
Risk and Performance-Based Auditing	54
Implementation of Upcoming Standards	55
PER-003-1 Operating Personnel Credentials	55
FAC-008-3 Facility Ratings	55
FAC-013-2 Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon	55
Actively Monitored List	56
Appendix A – Actively Monitored Reliability Standards	57
Appendix B – Compliance Audit Observation Report of Regional Entities	60
Introduction and Audit Oversight Objectives	60
Selection Criteria	60
2011 AAO Oversight Results	61
Positive Observations	61
Status Update (Debrief) Tool	61
Daily Caucus and RSAW review with the Audit Team	61
Enforcement Turnover	61
Just in Time Training	62
Recommendations to the Audited Registered Entity	62
Cross-training CIP auditors	62

FAC-008 and FAC-009 Facility Rating Methodology Checklist.....	62
Index Tool for Evidence Identification	62
Interview Tracking Tools	62
Lessons Learned	62
Disjointed Documentation:.....	63
Suggestions and Items for Consideration	63
Same Corporate Umbrella - Auditing Multiple Registered Entities (different NCR numbers and entity names)	63
Including Guidance within the Audit Notification Packet	63
Use of a daily debrief or status update tool	63
Interviewing Techniques.....	64
Responsible Person for Presenting Evidence.....	64
Critical Infrastructure Department (CID)	64
Technical Feasibility Exceptions (TFEs)	65
Sufficiency	65
Auditor Training Activities	66
Appendix C – Regulatory Actions.....	67

Executive Summary

This report provides details, analysis, lessons learned, and forward-looking activities regarding the Electric Reliability Organization's (ERO) implementation of the Compliance Monitoring and Enforcement Program (CMEP) in 2011. The information for this report was collected from the eight Regional Entities (RE) and North American Electric Reliability Corporation (NERC) staff. Specific areas where information was received from NERC staff include the Compliance Operations department's Audit Assurance and Oversight (AAO), Compliance Interface and Outreach, and Organization Registration and Certification groups, the Reliability Risk Management department's Event Analysis (EA) and Investigation Teams and Human Performance groups, the Standards Development group, the Compliance Enforcement department, the Critical Infrastructure Department, and the Legal and Regulatory department. In early 2012, the REs provided NERC information about their programs via a survey

NERC Staff CMEP Activities

The NERC staff's CMEP activities included the initial steps undertaken to ensure that NERC's risk-based approach was interated in an effective and efficient manner within NERC's Compliance Operations and Compliance Enforcement departments in 2011. The specific challenges and accomplishments faced by NERC staff are described as follows:

- NERC, with input from the REs, continued to use and develop Compliance Application Notices (CANs). The purpose of the CAN is to create consistency regarding how compliance is being assessed in the field. In 2011, 25 final CANs were posted on the NERC website and four CANs were retired.¹
- NERC, with input from the REs, released four Compliance Application Reports (CARs). CARs provide a thorough analysis of reliability standards that have a high frequency of violations, in order to help registered entities and REs understand why certain standards are so frequently violated. Additionally, based upon analysis of these violations, lessons learned are provided to aid the industry in compliance.²
- NERC issued seven Public Notices in order to provide additional compliance information on a variety of issues. Of particular note, was the Transfer of Assets and Deployment of New Assets bulletin. It clarified the effects of bulk power system (BPS) asset transfers or deployment of new BPS assets, as they relate to a registered entity's responsibility for compliance with the applicable NERC Reliability Standards, upon taking possession or commencing operation of these assets.³
- NERC conducted a Key Reliability Standard Spot Check (KRSSC) Program to analyze and promote the consistency of the REs audit approaches with the reliability standards. PRC-005 was the first reliability standard selected in 2011 to evaluate the RE audit approaches.⁴ The KRSSC Program will be used to inform the standards development

¹ Compliance Applications Notices are located at: <http://www.nerc.com/page.php?cid=3%7C22%7C354>

² Compliance Analysis Reports are located at: <http://www.nerc.com/page.php?cid=3|329>

³ Public Notices are located at: <http://www.nerc.com/page.php?cid=3|22>

⁴ KRSSC of PRC-005 information located at: <http://www.nerc.com/files/PRC-005-1%20KRSSC%20Final%20Report-%2009142011.pdf>

process of needed areas for improvements in terms of compliance monitoring and used in any revised audit approaches as related to the Reliability Standards Audit Worksheets (RSAWs).

- NERC, with input from the REs, developed a new Administrative Citation Notice of Penalty format that was used during the first eight months of 2011. The Administrative Citation Notice of Penalty format was discontinued as a result of the Compliance Enforcement Initiative. Two new formats for reporting the disposition of Possible Violations were utilized beginning in September 2011. These included the Spreadsheet Notice of Penalty (NOP) format and the Find, Fix, Track and Report (FFT) spreadsheet format.⁵ The key objective of the Compliance Enforcement Initiative (CEI) is to align ERO processing of Possible Violations (PVs) to the level of risk posed to the reliability of the BPS.⁶
- In order to enhance and develop the technical and auditing capabilities of Compliance Enforcement Authority (CEA) staff, NERC conducted four Lead Auditor training sessions and two CIP Standards training sessions for auditors. Additionally, ERO staff (NERC and the REs) completed two ERO CEA staff workshops. The purpose of these workshops was to provide auditors with CMEP information and updates and to ensure consistency in the application of the program across the industry.⁷
- NERC staff attended and made presentations at 18 RE compliance workshops to provide guidance to registered entities and to receive information that can be used to improve the CMEP going forward.
- NERC processed two appeals⁸ and certified 10 registered entities, bringing the NERC Compliance Registry to a total of 1,914 registered entities that are registered for 4,722 functions.⁹ The registration and certification process ensures that those entities that have material impact on the BPS are properly registered as a user, owner, or operator of the BPS.

Regional Entities CMEP Activities

REs were asked to provide insight into their compliance monitoring, outreach, and enforcement programs, effectiveness of their CMEP, events analysis and compliance review processes, and to describe the metrics they are using and where they see their programs in the future. Each of these issues is addressed in turn below:

- The REs reported that self-identified violations, i.e. those identified through self-reports and self-certifications, continue to be the leading method in which PVs are identified. Self-identified discovery methods accounted for 67% of all violations discovered in 2011, which is a slight increase from the 65% recorded in 2010. This continuing trend demonstrates the growth and maturity of internal controls within registered entities' compliance programs throughout the industry.

⁵ See the searchable Find, Fix, Track and Report (FFT) spreadsheet at: <http://www.nerc.com/filez/enforcement/index.html>

⁶ Filing of Compliance Enforcement Initiative is located at: <http://www.nerc.com/page.php?cid=1|9|170>

⁷ ERO auditor training information is located at: <http://www.nerc.com/page.php?cid=3|23|378>

⁸ Decisions on Appeals are located at: <http://www.nerc.com/page.php?cid=3|25|172>

⁹ Organization Certification information is located at: <http://www.nerc.com/page.php?cid=3|25|294>

- Several REs reported that improved data transmission processes between the audit team and registered entity have resulted in a significant reduction to the man-hours required to complete an audit.
- Each RE reported that the use of metrics have been very valuable. The most common metrics being monitored include: tracking of audits, spot checks, Notice of Violations, mitigation plans, budgeting constraints, and resource planning. Going forward, the ERO Compliance and Enforcement Management Group (ECEMG) has taken on the project of ensuring and improving metric consistency between the REs.
- The newly instituted Actively Monitored List (AML) tiered approach is being found as beneficial in that the process identifies those standards and requirements that have a direct impact on the reliability of the BPS reducing audit scope and ultimately lowering audit burden.¹⁰
- The Administrative Citation Notice of Penalty process and subsequently the CEI FFT and new NOP formats brought efficiency gains to the REs. The FFT process ensures all PVs are addressed and helps focus resources on those risks that have the greatest impact to reliability of the BPS, thereby advancing NERC's risk based approach to each regional CMEP.
- The eight REs reported that they completed all scheduled 2011 audits, representing 451 compliance audits of registered entities.¹¹
- The eight REs reported that they were on track for a timely completion of their six year audit cycles.
- In 2011, REs conducted a total of 26 compliance seminars and workshops reaching out to approximately 4,365 participants and developed newsletters and several other forms of outreach to the industry.
- REs reported that registered entities completed 303 event analysis self-assessments in 2011.

Significant 2011 Projects

NERC pursued several significant projects throughout 2011. These projects have had the primary focus of streamlining and more closely associating CMEP efforts to a risk-based process such that identified areas of BPS reliability risk are those that have the greatest time and effort dedicated to them. The ERO activities that have been developed at NERC and implemented by the REs and NERC to realize this goal are described as follows:

- As directed by FERC, in 2011, NERC formally defined the Bulk Electric System (BES) to ensure consistency between the REs and clarity of components contained therein.¹² The filing is pending at the Commission. This could limit the facilities that are subject to NERC Reliability Standards and therefore have an impact on compliance monitoring processes.

¹⁰ 2011 Actively Monitored Reliability Standards list is located at: <http://www.nerc.com/commondocs.php?cd=3>

¹¹ One audit with a non-FERC jurisdictional entity was postponed for one year.

¹² Details on defining the Bulk Electric System can be found at: http://www.nerc.com/filez/standards/Rules_of_Procedure-BES.html

- A significant change in the paradigm for monitoring and enforcing compliance with reliability standards was set into motion in 2011 with the FFT process. After several years of experience with the current program, FERC agreed that NERC and the Regional Entities should have the flexibility to more efficiently process and track lesser risk violations in order to focus their resources on issues that pose the greatest risk to reliability.¹³
- NERC and the Regional Entities began work on a registered entity assessment template. This assessment is being developed to establish a consistent basis for appropriately scoping compliance monitoring, to provide an opportunity for Regional Entities to work with registered entities on reliability efforts, and for registered entities to showcase their reliability efforts.
- To create a proactive focus on reducing human error and those precursory factors that allow human error to impact system reliability and to lower externally identified violations, NERC initiated a human performance program.
- To allow a registered entity to better analyze enforcement data, the Compliance Enforcement department developed the NOP searchable spreadsheet.¹⁴ This tool provides a means for any entity to quickly compare and contrast ERO-wide data with regards to penalty specifics.
- The CAN process was revised to clarify that a CAN provides instructions to CEA staff regarding compliance assessments of registered entities with applicable reliability standard requirements. Additionally, the process was revised to include a high level of review mechanism to address concerns raised with a given CAN.¹⁵
- In response to a number of registered entities within the Western Interconnection, NERC granted time for all entities subject to the Rated System Path Methodology standard MOD-029-1a requirement (R) 2.1.
- NERC incorporated a stronger focus on risk-based and performance-based criteria into the ERO audit approach for 2012 in the August 2011 AML revision.¹⁶
- To foster consistency across the REs, NERC held two ERO auditor workshops for CEA Staff in 2011. The purpose of the ERO CEA Workshops is: 1) to increase the competency level of the CEA Staff and 2) to improve consistency in the application of the CMEP across the ERO. The workshops included presentations, panel discussions, and breakout work sessions, which provided CEA staff the opportunity for interactive involvement and continuing training.¹⁷

¹³ See the searchable Find, Fix, Track and Report (FFT) spreadsheet at: <http://www.nerc.com/filez/enforcement/index.html>

¹⁴ See the searchable Notice of Penalty spreadsheet at:
http://www.nerc.com/filez/enforcement/Searchable_Enforcement_Page_03052012.xlsx

¹⁵ The CAN process procedure can be found at: <http://www.nerc.com/files/CAN%20Process%20Version%205.pdf>

¹⁶ See 2011 Actively Monitored Reliability Standards at: <http://www.nerc.com/commondocs.php?cd=3>

¹⁷ See NERC ERO Auditor Training page at: <http://www.nerc.com/page.php?cid=3|23|378>

Acknowledgement

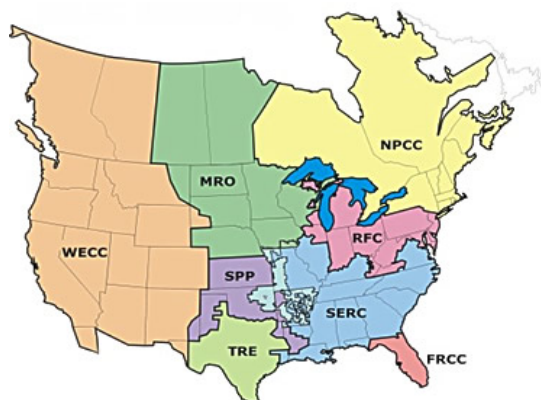
This report is the fifth annual report since NERC Reliability Standards became mandatory and enforceable in the United States (these reliability standards are mandatory in some Canadian provinces). An annual report is developed following the conclusion of the program at each year end, allowing for the evaluation of program activities for a complete year. NERC collects this information from the REs in the first quarter and develops a draft report for review by the REs, the Compliance and Certification Committee (CCC), and the Board of Trustees Compliance Committee (BOTCC).

Introduction

This report describes the results and effectiveness of the 2011 ERO CMEP as implemented by the eight REs through the Regional Delegation Agreements (RDA) and as overseen by NERC. FERC Order No. 672¹⁸ provides the framework for an ERO and its corresponding certification process. On July 20, 2006, FERC certified NERC as the ERO.¹⁹ FERC regulations provide that an ERO must submit an assessment of its performance three years from the date of certification by the Commission, and every five years thereafter. On September 16, 2010, FERC issued an order on NERC's three year performance assessment. Among other things, the Commission accepted "the performance assessment of NERC as the ERO, and the REs, and [found] that they continue to satisfy the statutory and regulatory criteria for certification."²⁰

On April 19, 2007, FERC approved eight RDAs²¹ through which NERC, as the international ERO, delegates certain compliance monitoring and enforcement activities ensuring that users, owners, and operators of the BPS in the United States comply with Commission-approved, mandatory reliability standards. In 2010, NERC negotiated modifications to the delegation agreements. The Commission-approved delegation agreements and associated orders by the Commission cover all aspects of the relationships between NERC and the REs, and provide an effective tool for oversight by NERC of the Regional programs and for managing those relationships. These REs include:

- Florida Reliability Coordinating Council, Inc. (FRCC)
- Midwest Reliability Organization (MRO)
- Northeast Power Coordinating Council, Inc. (NPCC)
- ReliabilityFirst Corporation (RFC)
- SERC Reliability Corporation (SERC)
- Southwest Power Pool Regional Entity (SPP RE)
- Texas Reliability Entity, Inc. (Texas RE)
- Western Electricity Coordinating Council (WECC)



The entities registered by the REs come from all segments of the electric industry including: investor-owned utilities, federal power agencies, rural electric cooperatives, state, municipal and provincial utilities, independent power producers, power marketers, and load-serving

¹⁸ See *Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 at P 31 (2006) at: http://www.nerc.com/files/20060720_ERO_certification.pdf

¹⁹ *Id.* at P 3

²⁰ See *Order on the Electric Reliability Organization's Three-Year Performance Assessment*, 132 FERC ¶ 61,217 at P 1 (2010) at: http://www.nerc.com/files/Order_on_NERC_Three_Year_Assessment.pdf

²¹ *North American Electric Reliability Council, et. al., Order Accepting ERO Compliance Filing, Accepting ERO/Regional Entity Delegation Agreements, and Accepting Regional Entity 2007 Business Plans*, 119 FERC ¶ 61,060 (2007). The RDAs can be found on the NERC website at: <http://www.nerc.com/page.php?cid=1|9|119|181>

entities. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

The RE and NERC Compliance staffs work together to improve consistency across all RE compliance activities, increase communications and collaboration for ERO implementation, and to identify any difficulties encountered, building an effective, consistently implemented, CMEP of the ERO and identify changes necessary for future years. The results of these efforts during 2011 are summarized in the Executive Summary and are detailed in the subsequent sections of this annual report.

Background

In 2007, there was a shift from voluntary compliance with industry-developed reliability standards to mandatory compliance with FERC-approved NERC Reliability Standards in the United States. NERC and the industry have worked intensively to transform decades of industry criteria, guides, policies, and principles into mandatory and enforceable NERC Reliability Standards in line with forces of change. A key turning point of the transformation stems back to 1996 when two major blackouts in the Western U.S. and the advent of open access transmission led NERC in 1997 to convene an independent “blue ribbon” panel (the electric reliability panel) and the U.S. Department of Energy to establish the Electric System Reliability Task Force, both groups to advise on critical institutional, technical, and policy issues necessary to maintain BPS reliability.

Both groups:

- Determined grid reliability rules must be mandatory and enforceable to ensure reliability in an increasingly competitive marketplace;
- Recommended the creation of an independent, ERO to develop and enforce reliability standards throughout North America; and
- Stated that federal legislation in the United States was necessary to accomplish this goal.

As a result, NERC implemented the blue-ribbon panel’s recommendation by converting its planning and operating policies, principles and guides into planning standards. The NERC Board of Trustees (BOT) approved the reliability standards, setting the foundation for the voluntary compliance era with monitoring by NERC and the REs from 1999 through June 2007. On June 18, 2007, the first set of NERC Reliability Standards became mandatory and enforceable in the United States. Of note, in 2002, NERC operating policies and planning standards became mandatory and enforceable in the Canadian province of Ontario.

CMEP Process

NERC and the REs continuously balance the interest in the United States to improve transparency with the confidential nature of the CMEP processes. Figure 1 is a pictorial view of the compliance process and shows how most of the processes in the CMEP fall under a window of confidentiality. NERC and the REs are continuously identifying and implementing innovative ways to share CMEP process information while honoring confidentiality requirements.

In 2010, NERC began publicly posting CMEP implementation and process information. NERC Compliance Operations has continued to review and publicly post CMEP implementation and process information in order to enhance the transparency of the CMEP and its implementation to registered entities.

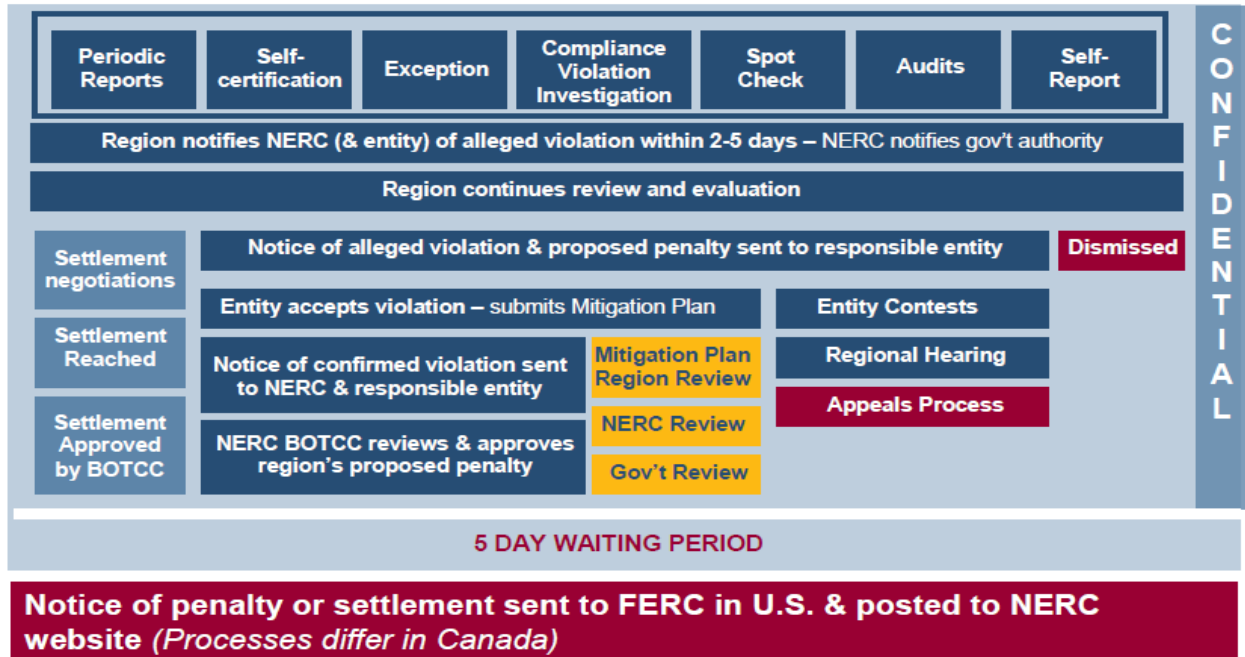


Figure 1: The CMEP Process.

NERC Staff CMEP Activities

This portion of the report provides an overview of the CMEP activities for 2011 that involved NERC staff who participated in the CMEP.

Compliance Operations Department

The Compliance Operations Department is charged with the overarching goal of ensuring the success of the REs and registered entities with respect to reliability compliance. The Compliance Operations Department is comprised of the following groups: Audit Assurance and Oversight, Compliance Interface and Outreach, and Organization Registration and Certification.

Audit Assurance and Oversight Group

The Audit Assurance and Oversight (AAO) group participated on a number of fronts to help ensure and promote the BPS. Most notably, AAO provided oversight to the RE for six compliance audits of registered entities. A compliance application is an issue that relates to a particular application of a reliability standard that may require additional scrutiny within the ERO in addition to guidance in the form of a Compliance Application Notice (CAN) or otherwise to ensure consistent application. From these oversight activities, NERC identified 11 potential compliance applications that were shared with the NERC Reliability Standards department for future reliability standard revisions and consideration for CAN development. The AAO compliance auditors identified 13 positive observations, one lesson learned and made nine recommendations to ensure the effectiveness and consistency of Regional audit teams as they perform compliance monitoring activities within the ERO. Positive observations, recommendations and lessons learned from the 2011 RE compliance audits attended by the AAO staff were presented to the eight RE compliance auditors at the ERO Compliance Workshop, in February of 2012.²² Oversight findings were communicated to the RE compliance auditors at the ERO Compliance Auditor Workshop, the Compliance Monitoring Program Working Group (CMPWG) and individually to the applicable RE Audit Team Lead.

Another measure promoting reliability include the AAO's support of the standard development process in the drafting of FAC-003-2 Transmission Vegetation Management.²³ For this standard, AAO provided peer review of the standard's ability to be effectively audited and to identify potential areas of concern.

AAO assisted in the review of, and proposed solutions to industry feedback regarding technical implementation concerns on MOD-029-1a's Rated System Path Methodology and its impacts on available transfer capability. This resulted in the development of a public bulletin titled "Rated System Path Methodology – Compliance Extension Request".²⁴

²² ERO Compliance Workshop information is posted on the NERC website at: <http://www.nerc.com/page.php?cid=3|23|378>.

²³ FAC-003-2 is FERC approved and posted on the NERC website at: <http://www.nerc.com/files/FAC-003-2.pdf>.

²⁴ This bulletin can be found on the NERC website at: <http://www.nerc.com/files/DRAFT%20Bulletin%202011-00X%20MOD-029-1a%20Compliance%20Extension%2020110718%20FINAL%20for%20Posting.pdf>.

In 2011, the AAO group developed several strategic programs to ensure accountability and oversight of REs' implementation of the CMEP. Of note are programs to address FERC feedback of RE compliance audits and closure of Event Analysis items being completed by the REs.

AAO participated in conference calls with FERC staff whereby FERC observers provided its feedback of the compliance audits performed by the REs. The AAO developed a FERC Feedback Tracking Process, capturing FERC issues for resolution. In 2011, NERC tracked and addressed 82 FERC observations identified in both Planning and Operations and CIP compliance audits. These observations included positive items and areas of improvement. The AAO team is capturing these lessons learned and sharing them directly with the applicable RE and will be providing training to the eight REs in the ERO staff workshops.

AAO developed a transition process and procedure between the Event Analysis (EA) department and AAO. This process assures oversight of RE's completion of compliance activities stemming from events or investigations which occurred on the BPS.

The AAO team provided NERC oversight of the Western Electricity Coordinating Council (WECC) spot check of Turlock Irrigation District (TID or Turlock) and Modesto Irrigation District (MID or Modesto). This spot check was performed in accordance with FERC Order from March 17, 2011 NP10-18-000.²⁵ NERC and WECC reported to FERC the results of the spot checks in accordance with the FERC order.

The Compliance and Certification Committee (CCC), a NERC BOT stakeholder committee, is tasked with assuring NERC's compliance with the rules of procedure (ROP).²⁶ The AAO team provided its support and expertise to the CCC in its development of RE Program Evaluation Procedure-CCCPP-010, approved by the NERC BOT. The CCCPP-010 criteria will be used in the 2012 AAO oversight of the REs performance, per ROP section 402.1.2.²⁷ AAO also supported the NERC staff for the CCC spot check of the NERC compliance monitoring and enforcement program and provided audit team lead training to the CCC auditors.

The AAO department produces this CMEP Annual Report, which provides a report on CMEP activities completed by NERC and the REs for the prior year. AAO developed and posted the 2010 and 2009 CMEP Annual Report in 2011.²⁸

In addition, AAO participated in the first FERC performance audit of PJM in 2011.

Risk-Based Approach

The AAO group has undertaken a number of projects to bring about a risk-based approach to compliance monitoring. Foremost in these efforts is the AML of reliability standards for 2011.²⁹

²⁵ See "Order on Review of Notice of Penalty", 134 FERC ¶ 61,209 at P 53 and Ordering Paragraph B ("March 17 Order").

<http://www.ferc.gov/whats-new/comm-meet/2011/031711/E-3.pdf>

²⁶ Information regarding the CCC can be found on the NERC website at: <http://www.nerc.com/page.php?cid=19|117|125>

²⁷ See NERC ROP Section 402.1.2,

http://www.nerc.com/fileUploads/File/Rules_of_Procedure/NERC_Rules_of_Procedure_EFFECTIVE_20120110_without_appendices.pdf

²⁸ The CMEP Annual Reports are located at the following link: <http://www.nerc.com/page.php?cid=1|8>.

²⁹ <http://www.nerc.com/commondocs.php?cd=3>

The AML has been completely redeveloped and reformatted to embody a three tiered approach. In this tiered approach, the requirements of a set of high priority reliability standards have been divided into three tiers based upon their relationship to the risk and potential impact to the reliability of the BPS. The requirements with the greatest potential risk and impact have been designated as Tier 1 and are designated as the minimum audit scope for all compliance activities occurring in 2012. Tiers 2 and 3 represent the requirements that are still significant to reliability, but have a less direct link in terms of actual performance or activities that registered entities carry out in support of reliability.

Another of these projects is AAO's support of the Compliance Enforcement Initiative (CEI).³⁰ Specifically, AAO has contributed to the data analysis and the auditor training program included in the CEI in order to ensure that Regional audit staff is prepared to identify and assist registered entities in their mitigation of lesser risk issues to the BPS. In addition, AAO has helped to lead the effort in the development of a registered entity risk profile assessment. This assessment will assist the ERO in its determination of appropriate audit scope based upon a number of risk related factors embodied by a registered entity, taking into account physical assets, internal controls, and compliance history among other things as part of the assessment. Audit Team Lead Training was revised to include training on the risk profile assessment.

The AAO department supported multiple projects within and outside the Compliance Operations arena to enhance and meet the corporate objective of a learning organization. AAO provided technical expertise in the development of CANs, bulletins and CARs. AAO developed two webinars to educate the stakeholders and REs compliance auditors on the 2012 AML. AAO developed and presented multiple topics at the spring and fall ERO Compliance Auditor workshops and responded to 50 compliance related questions from the stakeholders. AAO also provided Audit Team Leader Training on four times throughout 2011.

Seminars and Communications

In 2011, NERC presented three webinars to the industry as well as to the RE staffs. The topics for the webinars included registration options (JROs, CFRs, individual organization registration) as well as certain aspects of the Certification process, including the use of a Master Matrix in connection with the appropriate function (RC, BA or TOP) questionnaire to confirm an entity has the tools, processes, training, procedures and personnel to demonstrate its ability to meet the requirements of performing these critical functions.

Auditor Training Activities

The NERC compliance auditor training is generally based on the U.S. Government Accountability Office (GAO) Generally Accepted Government Auditing Standards³¹ (GAGAS) for performance audits. Throughout 2011, NERC conducted four sessions of the Fundamentals of NERC Compliance Audits for Lead Auditors training and two sessions of CIP Standards Training (CIP Basics for Auditors). The compliance auditor training material is continuously improved based on feedback from compliance audit experiences and changes to the GAO GAGAS, CMEP and

³⁰ Information on the CEI can be found on the NERC website at: <http://www.nerc.com/page.php?cid=3122>.

³¹ See GAO Government Auditing Standards available at: <http://www.gao.gov/new.items/d07731g.pdf>

NERC Rules of Procedure (ROP). Additional training modules, concerning GAO Auditing Standards, random sampling techniques, critical asset identification and a review of CIP-002 sufficiency reviews, for enhancing the CIP compliance auditor skills, were developed and offered in 2011.

NERC also regularly conducts a training class for NERC and RE staff who may lead Compliance Investigations (CIs). In 2011, NERC conducted three sessions of Fundamentals of CI Training. This training material is tailored for those who may lead CIs and is continuously being reviewed and improved based on feedback from CI experiences and changes to the GAO GAGAS, CMEP, NERC ROP and internal procedures.

Reliability Standard Audit Worksheets

The NERC RSAW are designed to add clarity and consistency to the assessment of compliance with reliability standards³². The RSAWs are used for multiple compliance monitoring methods. Comments on these and any of NERC's auditor resources are welcome and can be directed to the RE compliance managers.

The RSAWs are posted on the NERC public web site and provide information to the industry about expectations of the ERO compliance auditors when evaluating compliance with a reliability standard. NERC works in close coordination with the REs to ensure the information in existing RSAWs is updated with the latest regulatory authority language and guidance, and new RSAWs are developed as reliability standards are approved. It is recommended that REs and registered entities check the NERC website regularly to ensure the latest available versions of RSAWs are being used.

NERC works with REs to review these RSAWs on a continuous basis for improvement. NERC will transition the RSAWs into a database format in the near future to allow for timely updates as reliability standards are approved, modified, or retired.

Key Reliability Standards Spot Check

NERC concluded the first KRSSC of the eight REs regarding PRC-005 and posted the public report on September 14, 2011. NERC has initiated the second KRSSC of EOP-005. The purpose of this program is to compare and contrast the procedures and processes used across the eight REs when auditing a selected set of high risk or high impact reliability standards. Through this examination, NERC will be able to identify the issues Regional audit teams experience when evaluating compliance with the selected standards in addition to identifying the areas in Regional audit evaluations where additional guidance may be needed to improve evaluation processes or to promote consistency in evaluations. It is not an objective of this program to identify a minimum acceptable audit approach, but, instead, the focus will be on increasing the consistency and quality of audit approaches across all the REs.

³² The complete listing of RSAWs can be found at: <http://www.nerc.com/page.php?cid=3|22>

As an overview of the KRSSC program, NERC will request a sample of audits from all eight of the REs within a specified time period and conduct an in-depth analysis focused on selected reliability standards. Reliability standards selection will be based on:

- Severity Risk Index
- Compliance Statistics and Analysis
- Event Analysis review
- Stakeholder feedback
- NERC and Regional Entity Staff expertise

Each year, one standard will be selected for review. Performing this review will be a team of NERC auditors, who will examine non-public audit reports, completed RSAWs, and RE evidence in order to formulate any determinations. NERC will work with the Regional Entities to develop a notice to the industry to communicate lessons learned. In addition, NERC will work with the REs to improve audit procedures to respond to any consistency issues that may be identified.

Regional Entity Program Audits - Agreed Upon Procedures (AUP) Spot Check

In 2008, NERC developed the Agreed Upon Procedures Spot Check program for auditing the REs adherence to the NERC ROP, CMEP and its ERO functional responsibilities as defined in the Regional Entity delegation agreement. This was performed in accordance with FERC Order Numbers 672 and 672-A³³. Requirements concerning the RE audit program attributes including timelines are contained in the NERC ROP, Section 402.1.3 and Appendix 4A.

In 2010, NERC completed initial AUP audit activities of five of the eight REs (RFC, SERC, MRO, SPP RE and NPCC). NERC conducted the five audits using an independent contracting firm. The AUP approach allowed NERC to audit the REs adherence to the NERC ROP, CMEP, and the RDA requirements. Based upon experience gained and lessons learned in conducting the audits, NERC determined the audit process should be restructured to include more focus on risk and performance. With respect to the remaining three REs, NERC performed an analysis to assess the exceptions identified in the previous five audits performed. From this analysis, NERC developed a spot check audit process to verify that exceptions did not exist at the remaining three REs. NERC performed the spot check of TRE, WECC, and FRCC in the first quarter of 2011. The results of the AUP spot checks are posted at the NERC website.³⁴

Compliance Interface and Outreach Group

The Compliance Interface and Outreach group of the Compliance Opeartion Department has the primary responsibilities of developing guidance to REs and registered entities, which includes CANs and public notices.

³³ See *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

³⁴ See AUP Spot Check reports at <http://www.nerc.com/page.php?cid=3|26|349>

Compliance Application Notices

CANs were created by NERC, with input from the REs, to fulfill ERO obligations under FERC Order 693³⁵ to provide compliance guidance to CEA³⁶ staff and to provide transparency to industry in regard to compliance monitoring with NERC Reliability Standards. CANs encourage accountability for both CEAs and registered entities and were issued in response to requests for compliance guidance from industry stakeholders.

There are two significant and mutually reinforcing purposes of a CAN:

- To establish consistency in the application of compliance criteria across all CEAs; and
- To provide transparency to industry on how an ERO CEA will monitor compliance with a NERC Reliability Standard.

CANs are generated in a relatively short time period compared to a much lengthier formal standards development process. CANs not only assist CEAs in monitoring compliance, but the industry benefits from understanding what the issues are and how to prepare for an upcoming audit.

The CAN program was launched in 2010 and the following CANs were finalized through the end of 2011:

³⁵ FERC Order 693, Docket No. RM06-16-000.

³⁶ Compliance Enforcement Authorities include ERO auditors, investigators, enforcement personnel or any person authorized to assess issues of concern, potential non-compliance, and possible, alleged or confirmed violations of NERC Reliability Standard requirements.

Table 1: All Finalized Compliance Applications Notices	
CAN Number	Title
CAN-0005	CIP-002 R3 Critical Cyber Asset Designation for System Operator Laptops (revised)
CAN-0006	EOP-005 R7 Verification of Restoration Procedure (revised)
CAN-0007	CIP-004 R4.2 Revocation of Access to Critical Cyber Assets (CCAs) (revised)
CAN-0008	PRC-005 R2 Basis for First Maintenance and Testing Date (revised)
CAN-0009	FAC-008 and FAC-009 Facility Ratings and Design Specifications (revised)
CAN-0010	Implementation of Annual in Reliability Standard Requirements (revised)
CAN-0011	PRC-005 R2 Interval Start Date for New Equipment (revised)
CAN-0012	Completion of Periodic Activity Requirements During Implementation Plan (revised)
CAN-0013	PRC-023 R1 and R2 Effective Dates for Switch-On-To-Fault Schemes (revised)
CAN-0015	Unavailability of NERC Software Tools (revised)
CAN-0016	CIP-001 R1 Sabotage Reporting Procedure (revised)
CAN-0017	CIP-007 R5 Technical and Procedural System Access and Password Controls
CAN-0018	FAC-008 R1.2.1 Terminal Equipment (revised)
CAN-0020	TPL-002, TPL-003, TPL-004 & TOP-002 Equipment Outages
CAN-0022	VAR-002 R1 and R3 Generator AVR Operation in Alternative Mode (revised)
CAN-0024	CIP-002 R3 Routable Protocols and Data Diode Devices
CAN-0026	TOP-006 R3 Protective Relays (revised)
CAN-0027	TOP-003 R2 Coordination of Scheduled Outages
CAN-0028	TOP-006 R1.2 Reporting Responsibilities (revised)
CAN-0029	PRC-004 R1, R2, and R3 Protection System Misoperations
CAN-0030	Attestations
CAN-0031	CIP-006 R1 Acceptable Opening Dimensions
CAN-0039	EOP-004 R3 Filing DOE Form OE-417 Event Reports
CAN-0040	BAL-003 R2 and R5 Frequency Bias Calculation
CAN-0043	PRC-005 R2 Protection System Maintenance and Testing Evidence

In August of 2011, the NERC BOT instructed NERC to revise all existing CANs and to instruct auditors in the assessment of compliance instead of providing guidance for registered entities. The BOT also tasked NERC with revising the CAN process to allow for a high-level review mechanism, provide more opportunities for RE and industry feedback and prioritization and to outline the scope of CANs with relation to the current standard in effect.

As a result, several CANs were revised and they are indicated in the table above. The CAN Process document has also been updated and is posted on the NERC website.³⁷ NERC is committed to continuing and further developing the CAN program in 2012.

³⁷ CAN Process document can be found at: <http://www.nerc.com/files/CAN%20Process%20Version%205.pdf>.

Organization Registration and Certification Group

The purpose of the Organization Registration Program is to clearly identify those entities that are responsible for compliance with the FERC approved reliability standards. As described in the NERC ROP Appendix 5A *Organization Registration and Certification Manual*³⁸ NERC has established documented procedures to ensure a fair and impartial appeals process. From June 2007 to December 31, 2011, the ERO has processed 96 appeals, two of which were submitted in 2011 and 1 is still active at NERC. The REs have settled 65 and the BOTCC has processed 30. Four registration dockets remain open at FERC. The following figure 2 graphically illustrates the number of registered appeals that have been sought out each year and figure 3 provides the breakdown of these appeals by the applicable reliability function.

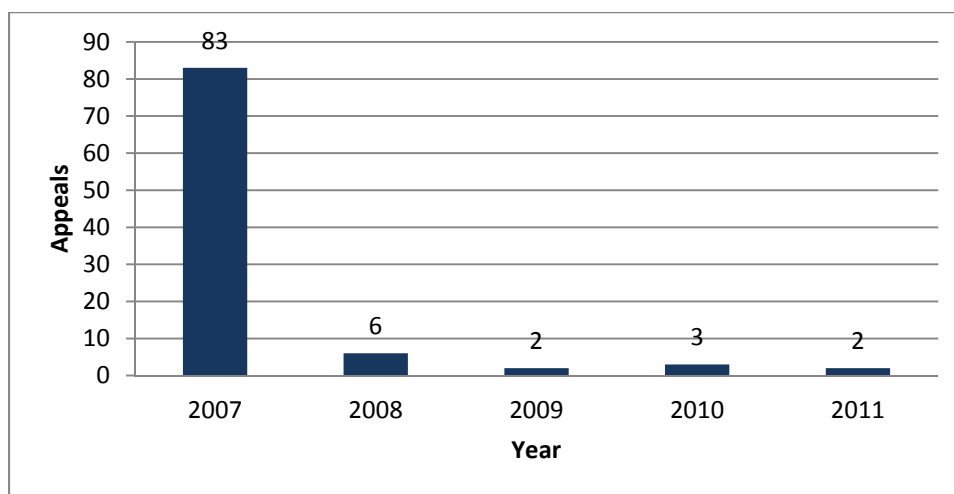


Figure 2: Registration Appeals by Year

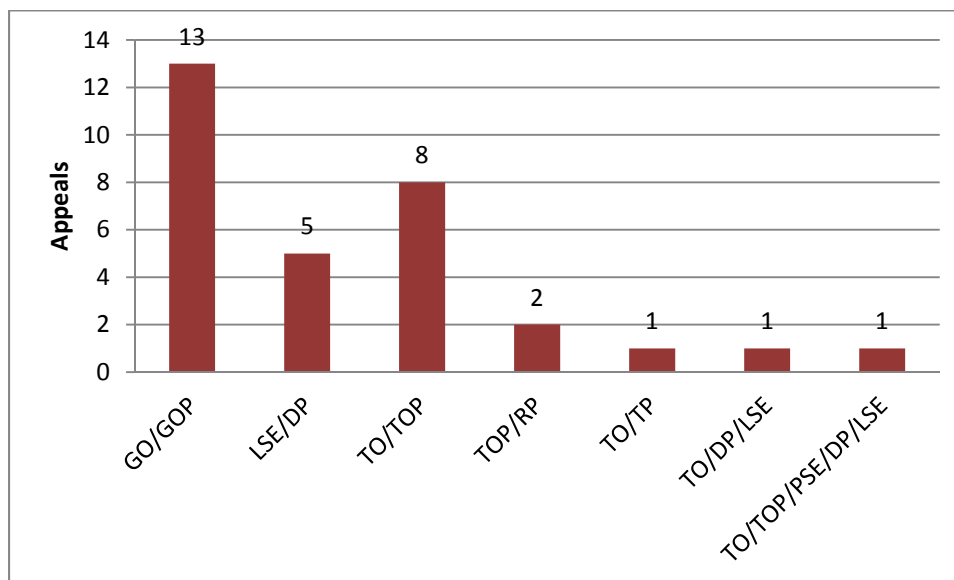


Figure 3: Registration Appeals by Function

³⁸ See Appendix 5A: *Organization Registration and Certification Manual* of the NERC ROP at: http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20110412.pdf

As described in the NERC Statement of Compliance Registry Criteria, NERC will include in its Compliance Registry (the NERC Compliance Registry or NCR) each entity that meets the specified criteria for a given function. Identifying these organizations is necessary and prudent at this time for the purpose of determining resource needs, both at the NERC and Regional Entity level, and to begin the process of communication with these entities regarding their potential responsibilities and obligations. In accordance with the NERC ROP, the NCR is updated on a monthly basis. As of December 31, 2011, NERC has registered 1,914 entities on the NCR for 4,722 registered functions.³⁹

The following details the entities per Region and by function. Also included is a summary of unique entities for each function.

Registration Status as of 12/29/2011

Summary of Registered Entities and Functions*

Region	Number of Registered Entities	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP	Total of Functions
ERCOT	218	1	46	108	88	1	58	1	42	1	1	0	30	16	28	1	422
FRCC	70	10	27	31	31	10	19	13	26	0	15	1	24	16	13	8	244
MRO	128	20	54	49	49	5	58	6	73	3	34	2	40	20	23	13	449
NCEA	3	1	0	0	0	2	0	1	0	2	1	0	0	1	0	1	9
NPCC	294	6	58	138	135	6	59	6	86	5	6	2	29	14	15	13	578
RFC	349	12	69	155	151	3	54	3	161	2	15	1	38	14	12	3	693
SERC	254	32	80	104	99	28	80	21	88	8	31	7	51	27	31	17	704
SPP	133	17	48	56	54	2	49	1	65	1	24	1	40	18	20	5	401
WECC	465	33	171	214	209	1	145	29	146	1	54	3	85	53	44	34	1,222
Totals	1,914	132	553	855	816	58	522	81	687	23	181	17	337	179	186	95	4,722

Summary of Unique Entities and Functions**

Unique Entities	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP	Unique Functions
1,641	128	544	835	796	51	512	74	445	16	176	13	334	176	179	89	4,368

Table 2: Registration Summaries

Multi-Regional Registered Entity (MRRE)

Initially, NERC determined to implement a program of registering entities under a Multiple Region Registered Entity (MRRE) program. Due to a number of logistical reasons, the program was temporarily suspended. Since its suspension however, a number of entities registered in multiple Regions have approached NERC to reconsider its approach. NERC, with input from the Regional Entities, is in the process of evaluating such a program. The Regional Entities are performing joint audits for many entities that are registered in multiple regions. Other processing activities are also being considered.

³⁹ The NCR can be found on NERC's website at: <http://www.nerc.com/page.php?cid=3|25>

Organization Certification

The purpose of the Organization Certification Program is to ensure that a Reliability Coordinator (RC), Balancing Authority (BA), or Transmission Operator (TOP) has the tools, processes, training, procedures and personnel to demonstrate its ability to meet the requirements of all applicable reliability standards applicable to its function(s). Both NERC and the Regional Entities have specific roles and responsibilities regarding organization certifications pursuant to the NERC ROP Section 500 and Appendix 5A and the Organization Registration and Certification Manual.

NERC expects that the number of certifications, approximately ten per year, will remain about the same due to mergers, acquisitions, future agreement and market changes.⁴⁰

Listed below in Table 3 are the 10 entities that were certified in 2011 along with their associated RE and the applicable functions receiving certification.

Table 3: 2011 Certified Registered Entities		
Registered Entity	Regional Entity	Function
Public Utility District No. 1 of Clark County	WECC	TOP
City of Springfield	SPP	BA
Mesquite Power, LLC	WECC	TOP
PJM Interconnection, LLC	RFC	BA, RC, TOP
Horse Hollow Generation Tie, LLC	TRE	TOP
New Harquahala Generating Company, LLC	WECC	TOP
Arlington Valley	WECC	TOP
City of Lansing by its Board of Water and Light	RFC	TOP
Hetch Hetchy Water and Power	WECC	TOP
Silicon Valley Power	WECC	TOP

GO/TO Directive

Entities that use, own or operate elements of the BES are (i) owners, operators, and users of the BPS and (ii) candidates for registration for applicable functions. Using the registry criteria, New Harquahala (NH) was registered as a TO/TOP. NH appealed and the final ruling from FERC upheld this registration. This registry and appeal prompted formation of an Ad Hoc Group to study the registration of generation owners and operators that own and operate transmission facilities. The Ad Hoc Report:

⁴⁰ Certification final reports are can be found at: <http://www.nerc.com/page.php?cid=3|25|294>

- Recommended changes to requirements:
 - 32 requirements - add Generator Interconnection Facility to requirement
 - 12 requirements in FAC-003-1
 - 2 requirements – expand applicability to GO/GOP
 - 8 new requirements
- Recommended changes to compliance registry
- Recommended changes to definitions
- Recommended adding 2 new terms; and revising 5 existing terms
- Concluded “Don’t register GO as TO/ or GOP as TOP solely based on Generator Interconnection Facility” if the above recommendations were followed.

To date, three entities appealed WECC’s registration as TO/TOP to NERC and ultimately to FERC. These included: New Harquahala, Cedar Creek and Milford.

In each case, the NERC BOTCC and FERC upheld the registration of the entities as TOs and TOPs. Requests for rehearing and a compliance filing remains pending before the Commission.

The FERC orders made clear:

- There is an apparent gap in reliability
- All GO or GOPs or both do not have to be registered as TO or TOPs or both
- Limited set of Standards could be required and NERC was encouraged to develop a mechanism to accomplish this

In response to the report from the Ad Hoc Group, a Standard Development Team was formed (Project 2010-07) to determine which course to take to resolve FERC’s concern in the apparent gap in reliability and determine the guidelines for GOs and or GOPs that own or operate a transmission facility.

Parallel to the efforts of the Project 2010-07 SDT, NERC Staff developed an interim measure intended to limit the number of GOs/GOPs that would be registered prior to revising the appropriate standards, and to provide guidance as to a limited sub-set of requirements that would apply to those that were registered as TO/TOP.

As of the end of 2011, efforts of both the Standard Drafting Team (SDT) and NERC Staff have been suspended waiting on the Board of Trustees consideration of the SDT submittal and FERC’s final ruling on the appeals of Cedar Creek and Milford.

Public Notices

NERC released in 2011 a Compliance Process Bulletin #2011-005 titled Transfer of Assets and Deployment of New Assets. This process bulletin was issued to clarify the effects of BPS asset transfers or deployment of new BPS assets as they relate to a registered entity’s responsibility

for compliance with the applicable NERC Reliability Standards upon taking possession or commencing operation of these assets.

Compliance Analysis Reports

NERC Compliance, with input from the REs, has conducted analyses of standards that have experienced a high frequency of violations since June 18, 2007. These analyses were developed in coordination with the REs, and were presented to the NERC BOTCC in the form Compliance Analysis Reports (CARs).⁴¹ The purpose of these reports is two-fold. First, they provide information and a way to consider the most violated standards. Second, they serve as a formal mechanism to provide feedback to the standards development teams as they evaluate the requirements of a specific standard based upon compliance experience. In 2011, five CARs were released and covered the following processes:

EOP-005 – System Restoration Plans

Since the beginning of the mandatory and enforceable standards on June 18, 2007, EOP-005 has been one of the Top 10 violated standards. As of April 1, 2011, there are 128 active or closed violations of EOP-005-1. EOP-005-2 standard was approved by FERC on March 17, 2011 with an effective date of July 1, 2013. The goal of the report was to aid REs in lessons learned for compliance with EOP-005-1.

TOP-002 – Facility Ratings Methodology

There are three main reasons TOP-002 was chosen for a CAR:

- TOP-002 is the 4th most violated non-CIP standard, all-time;
- TOP-002 is the 5th most violated non-CIP standard in the last 12 months; and
- TOP-002 is applicable to over 63% of Registered Entities.

Self-reports and self-certifications of this standard account for 74% of the violations. This metric shows an active and aggressive compliance monitoring program and a good internal compliance program.

In this CAR, in addition to a rigorous analysis of the associated data, suggestions were offered for Industry consideration to help reduce the number of violations.

VAR-002 - Generator Operation for Maintaining Network Voltage Schedules

As a result of the initial CAR on VAR-002-1.1b dated August 2010 and further discussion, this CAR has an addendum added to clarify the location of the point of measurement for the Transmission Operator voltage schedule.

NERC Organization Certifications

This was the first analysis report on the NERC and the Regional Entity's Organization Certification Programs. This report provided a quantitative assessment of the thirty-five (35)

⁴¹ The complete list of CARs can be found at: <http://www.nerc.com/page.php?cid=3|329>

organization certifications completed June 2007 through the end of 2010. NERC plans to present this information annually to give an update regarding the previous year.

NERC Compliance Registry and Registration Appeals

Those on the NCR changes slightly each month as new entities are registered and others are deactivated as organizations change ownership. The lowest number of registered entities was 1,827 in May of 2008 and the highest number of registered entities was 1,940 in November of 2010.

At the time of the issuance of this report, the following was noted:

- “There are 36 registered JROs. One is in Texas RE, two are in FRCC, one is in MRO, 13 are in SERC, and 19 are in RFC. There are currently no JROs in NPCC, SPP or WECC. In the last six months, 12 new JROs have been registered with one Registered Entity entering into 11 different JROs for its DP and LSE functions in two different Regions.”
- “Currently, there are 46 CFRs comprising registrations for 144 entities and representing a total of 185 functions. While many entities are only registered in a CFR for one of its functions, some entities have two or more of its functions registered with multiple CFRs. The entities involved in CFRs in each Region are: 76 in Texas RE, 33 in MRO, 19 in RFC, 10 in SERC, two in SPP, and four in WECC. There are currently no CFRs in FRCC or NPCC. In the last six months, there have been two new CFRs for a group of 12 entities that entered into CFRs for their DP and LSE functions.”

Reliability Risk Management Department

The Reliability Risk Management Department combines the technical expertise of NERC’s system awareness staff, events analysis staff and event investigators to facilitate efficient processing of BPS events and to provide lessons learned to the industry to promote increased reliability of the BPS.

In the fourth quarter of 2011, the NERC Events Analysis and Investigations groups were combined with BPS Awareness into a single functional group designated as Reliability Risk Management (RRM). This new group’s mission is to ensure the reliability of the BPS by ensuring situational awareness of evolving events, conducting events analysis of events and occurrences; providing lessons learned and needed reliability industry alerts to industry stakeholders and addressing any resulting reliability concerns through interaction with Regional compliance staff. In addition, the investigations group may independently conduct compliance investigations as warranted.

The focus of RRM is to:

- capture credible system awareness information for BPS events and system conditions
- conduct robust event analysis using cause analysis and risk-based methods
- facilitate the gathering and dissemination of lessons learned and relevant reliability communications to industry stakeholders in a timely manner
- ensure appropriate level of compliance oversight for BPS events

On October 25, 2010, after considerable input from industry, REs, and regulators, the ERO enterprise initiated Phase I of a Field Trial.⁴² This voluntary process identified clear event categories, established associated levels of analysis and reporting and emphasized the importance of registered entities performing a systematic compliance self-assessment. In May 2011, Phase II of the Field Trial began with revised criteria for classifying events and expected responses from registered entities, Regional Entities and NERC based on information acquired during the earlier phase. Version 1 of the Electric Reliability Organization Event Analysis(EA) Process document was endorsed by the Operating and Planning Committees (PC) in January 2012; and approved by the NERC BOT on February 9, 2012. This version went into effect on February 21, 2012. While the components of the ERO Event Analysis Process – Version 1 document are not included in the NERC ROP, the program has been embraced by industry.

The ERO EA Process – Version 1 document process sets the expectation that entities will complete a preliminary event report. The higher the category of event, the more detailed analysis the registered entity is expected to perform and share with the Regional Entity and ultimately NERC. This significant amount of information, voluntarily provided by registered entities, has resulted in a significant reduction in the number of compliance investigations being initiated.

Additionally, the ERO EA Process – Version 1 document sets the expectation that registered entities should perform a critical self-assessment of standards and to develop a compliance self-assessment report proportional to the significance of the event or risk to the BPS. Since the start of the field trial through the end of 2011, there were 220 qualified events. registered entities conducted and shared their compliance self-assessments with Regional Entities in roughly half of these instances. In conjunction with these self-assessments, there were 15 self-reported violations of reliability standards.

Through the event analysis process, the Regional Entity compliance staff becomes aware of the event and engages with the registered entity to establish a time table for the compliance self-assessment by the entity. Upon receipt of the entity self-assessment, the Regional Entity prepares an evaluation of the event compared against relevant standards and shares that with NERC. In situations where formal compliance monitoring is indicated, the follow-up is done by the Regional Entity.

In 2011, the Bulk Power System Awareness (BP-SA) Group published nine NERC Alert Advisories and coordinated response activities for two NERC Alert Recommendations. Additionally, BP-SA coordinated Crisis Action Plan conference calls with the REs and governmental entities for high impact low frequency events like the April tornados in the South, the hurricane in August and the Northeast Snowstorm in October. NERC triaged over 950 BPS events and occurrences and publish 22 lessons learned,⁴³ operational experience reports,⁴⁴ and reminders to the industry.⁴⁵

⁴² See *Electric Reliability Organization Event Analysis Process: Field Test Draft* at:

http://www.nerc.com/docs/eawg/Event_Analysis_Process_Field_test_DRAFT_102510-Clean.pdf

⁴³ Lessons Learned from the EA&I group are available at: <http://www.nerc.com/page.php?cid=5|385>

⁴⁴ Operational Experience Reports, otherwise known as System Disturbance Reports, are available at: <http://www.nerc.com/page.php?cid=5|66>

⁴⁵ Reminders to the Industry in the form of NERC Alerts are available at: <http://www.nerc.com/page.php?cid=5|63>

In addition to the contribution made to event analysis during 2011, the Reliability Risk Management (RRM) group:

- Completed five NERC-led CIs
- Participated in four Regional Entity-led CIs
- Initiated no NERC-led CIs

Human Performance

NERC has initiated a human performance program, to not only allow a more thorough analysis of the events on the BPS, but also to create a proactive focus on reducing human error and those precursory factors that allow human error to impact system reliability. The transfer of these important reliability messages requires a variety of instruments that can advise practices and training, particularly those that can affect the reliability of the BPS. Sharing across the North American industry allows expertise and experience to strengthen the grid as a whole, making everyone more successful in meeting reliability objectives. The techniques and procedures that NERC is using to propagate this initiative include conferences, workshops, webinars, and publications with facilitated active sharing among NERC and its stakeholders. A purposefully designed NERC sponsored Human Performance Conference is being planned for 2012 to address challenges related to human performance on the reliability of the BPS.

While human error is cited for a large part of the contributing causes for events on the BPS, the RRM is partnering with industry in the EA process and has initiated a new trending analysis system to assimilate the information received in entity reports. The process will aid in developing corresponding corrective action plans to address the causes of an event or failure and prevent reoccurrence of events by creating the databases needed to apply the principles of effective risk management. After an investigation, analysis, or determination of causal factors of any event, RRM studies the event or occurrence, often leading to the identification of root causes and causal factors that could drive larger events on the BPS. These processes are applied to all levels of the ERO enterprise, including NERC, the Regional Entities, and industry participants that conduct event analysis and are involved in corrective action programs when a cause analysis is required. This process is designed to be a companion process to the *Electric Reliability Organization Event Analysis Process Manual*. It is designed to assist those responsible for labeling and trending the causal factors and latent deficiencies leading to BPS events or failures.

Standards and Training Department

The number of standards has steadily grown since 2007. According to the 2011 AML, reviewed in Appendix A below, at the beginning of the year, the number of reliability standards reached 102. Of these 102 standards, registered entities were tasked with demonstrating compliance with 39 standards within compliance audits, 53 standards for self-certifications, one standard with spot checks, and 14 standards for periodic submittals.

Standards Development

Changes made to those reliability standards referred to as 693 standards, in reference to FERC Order No. 693, encompass six updates to existing standards and the implementation of seven

new standards. In terms of the CIP Standards, also referred to as 706 standards in reference to FERC Order No. 706, CIP-005-3 and CIP-006-3 underwent interpretations in 2011. Table four accounts for these standards and notes the date in which the standard became effective.

Table 4: 2011 Reliability Standards Changes

Standard	Effective	Standard	Effective	Standard	Effective
BAL-006-2	4/1/2011	IRO-006-WECC-1	7/1/2011	PRC-004-1a	9/26/2011
BAL-502-RFC-02	5/23/2011	IRO-008-1	10/1/2011	PRC-004-WECC-1	10/1/2011
CIP-001-2a	10/1/2011	IRO-009-1	10/1/2011	PRC-005-1a	9/26/2011
CIP-005-3a	2/2/2011	IRO-010-1a	10/1/2011	TOP-001-1a	11/21/2011
CIP-006-3c	5/19/2011	MOD-001-1a	4/1/2011	TOP-002-2b	10/20/2011
EOP-002-3	10/1/2011	MOD-004-1	4/1/2011	TOP-003-1	10/1/2011
FAC-002-1	10/1/2011	MOD-008-1	4/1/2011	TOP-005-2a	10/1/2011
FAC-501-WECC-1	7/1/2011	MOD-021-1	4/1/2011	TOP-006-2	10/1/2011
INT-003-3	4/1/2011	MOD-028-1	4/1/2011	TOP-007-WECC-1	7/1/2011
IRO-002-2	10/1/2011	MOD-029-1a	4/1/2011	TPL-002-0b	10/24/2011
IRO-004-2	10/1/2011	MOD-030-2	4/1/2011	VAR-001-2	10/1/2011
IRO-005-3a	10/1/2011	PER-004-2	4/1/2011	VAR-002-WECC-1	7/1/2011
IRO-006-5	7/1/2011	PER-005-1	4/1/2011	VAR-501-WECC-1	7/1/2011
IRO-006-EAST-1	7/1/2011	PRC-002-NPCC-1	10/20/2011		

Critical Infrastructure Protection Standards

The year 2011 continued to be an eventful year for the Critical Infrastructure Protection CIP standards. While a single version of the CIP Standards was in effect for the entire year, there was significant activity in future versions of the standards (*i.e.* the filing of Version 4 with FERC, FERC issuance of the Version 4 approval NOPR, and the initial posting and ballot of Version 5) which required significant attention from the Registered Entities. Throughout the year, the ERO continued the efforts for ensuring better compliance with the CIP Standards. These efforts are the following:

Transparency. The Critical Infrastructure Department (CID) worked jointly with REs to improve the consistency of compliance program results; improve risk-based approaches for auditing and spot checking; and promote a culture of security and compliance through education, transparency and incentives. Specifically, CID participated in 14 audits during 2011, all but one being observations of RE auditors as they assessed compliance of entities with the CIP standards. CID observers offered support to the audit team, bringing a perspective of consistency to interviews with subject matter experts, offering constructive feedback about auditing technique, or sharing lessons learned from other audits that focused on CIP Standards Requirements 002-009. In addition to the assigned CIP Oversight Audits of REs, the CIP auditors were engaged with the following programs and initiatives in 2011:

- Managed the Technical Feasibility Exception (TFE) program, to include interface with the Regional TFE managers and preparation of the annual report to FERC

- Coordinated and planned CIP Auditor Workshops
- Facilitated and provided administrative support to the CIP Compliance Working Group
Provided CIP subject matter expert presentations to Regional compliance workshops
- Provided CIP subject matter expertise (SME) and compliance liaison to the Cybersecurity 706 Standard Drafting Team
- Provided CIP subject matter expertise to the Situational Awareness for FERC, NERC, and the RE programs
- Provided subject matter expertise to NERC EA and Investigations
- Provided CIP subject matter expertise in response to queries from industry and the public, as submitted via NERC's web site
- Participated as a liaison for CIP compliance issues or concerns during weekly NERC and FERC status conferences

Uniformity. CID worked with the REs and industry to develop an objective basis for registered entities to identify critical assets for CIP-002, which was approved in 2010. Version 4 of the CIP reliability standards, which includes bright-line criteria, provides a specific list of assets for entities to consider critical, rather than having each entity develop a methodology to determine its critical assets. This significant accomplishment enables entities to more efficiently and effectively identify Critical Cyber Assets and deploy appropriate controls to protect those assets.

Sufficiency. CID continued to conduct the Sufficiency Review Program (SRP), an outreach to registered entities that examines the Risk-Based Assessment Methodology (RBAM) that is required by CIP-002-3. The SRP examines whether an entity's RBAM is sufficient to properly identify the Critical Assets that ensure the safe, reliable operation of the BPS. CID conducted ten SRP's in 2011.

Standards Development. The ERO continued the development of "Version 5" of the CIP Standards through the year. While the main focus of the Version 5 development was to address all the remaining FERC Order No. 706 directives, numerous other changes based on practical experiences from both registered entities and ERO audit staff (i.e. NERC and the Regional Entities) were included. In addition to the experiences provided by team members, the SDT held several informal meetings with both Regional CIP Audit Staff, and additional Registered Entity staff to better shape the standard prior to posting.

Enforcement Department

A graph of the number of violations in 2011 relative to the NERC Reliability Standards, Figure 4, provides a look at the twenty most violated reliability standards for 2011, highlighting the discovery method as either self-identified or externally discovered. Self-identified violations are violations that registered entities recognize within their own organization by way of self-reports, self-certification, periodic data submittals, and exception reporting. Externally discovered violations are those that are discovered by the ERO staff through compliance audits,

spot checks, complaints, and investigations. Eight of the top ten most violated standards in 2011 are CIP standards.

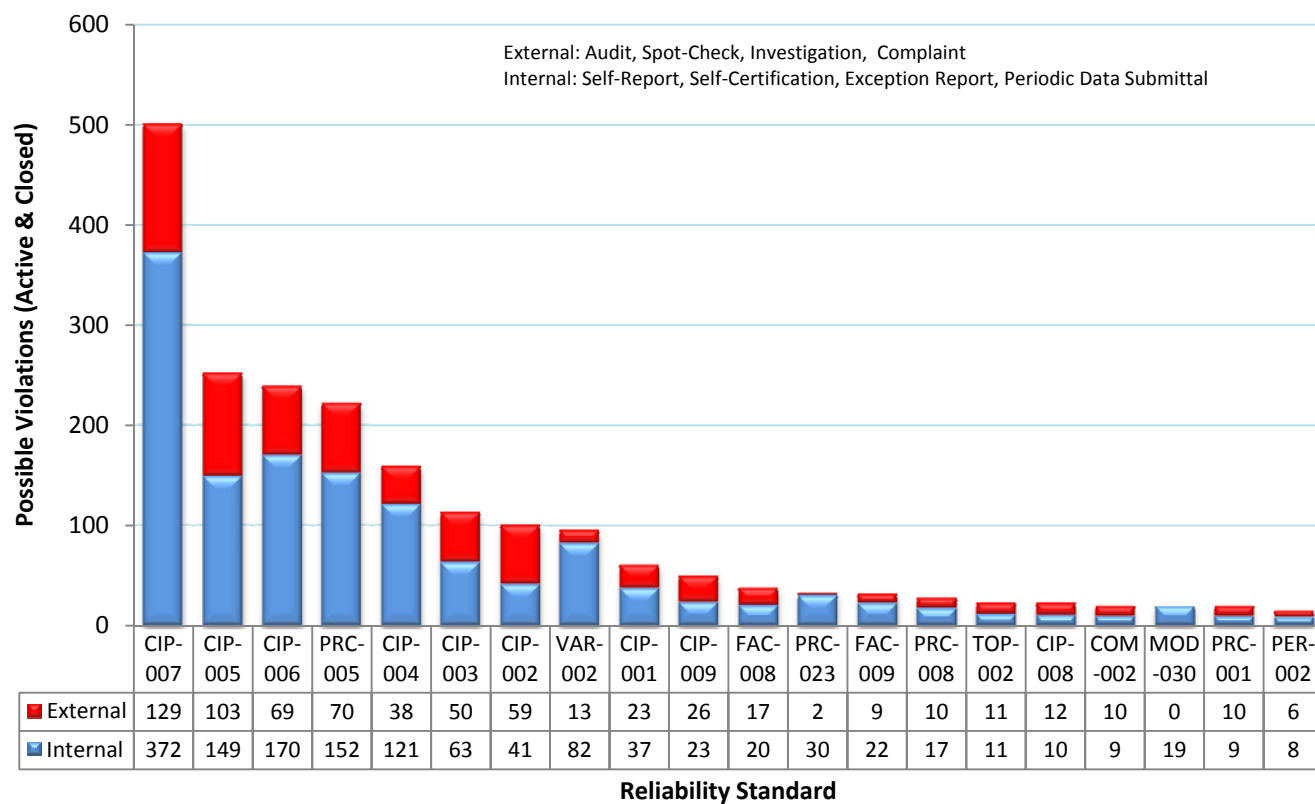


Figure 4: Top 20 Violated NERC Reliability Standards for 2011

In terms of the top twenty most violated standards for the period of June 18, 2007 through the end of December 2011, it is noteworthy that seven of the ten most violated standards are CIP standards, as shown in Figure 5.

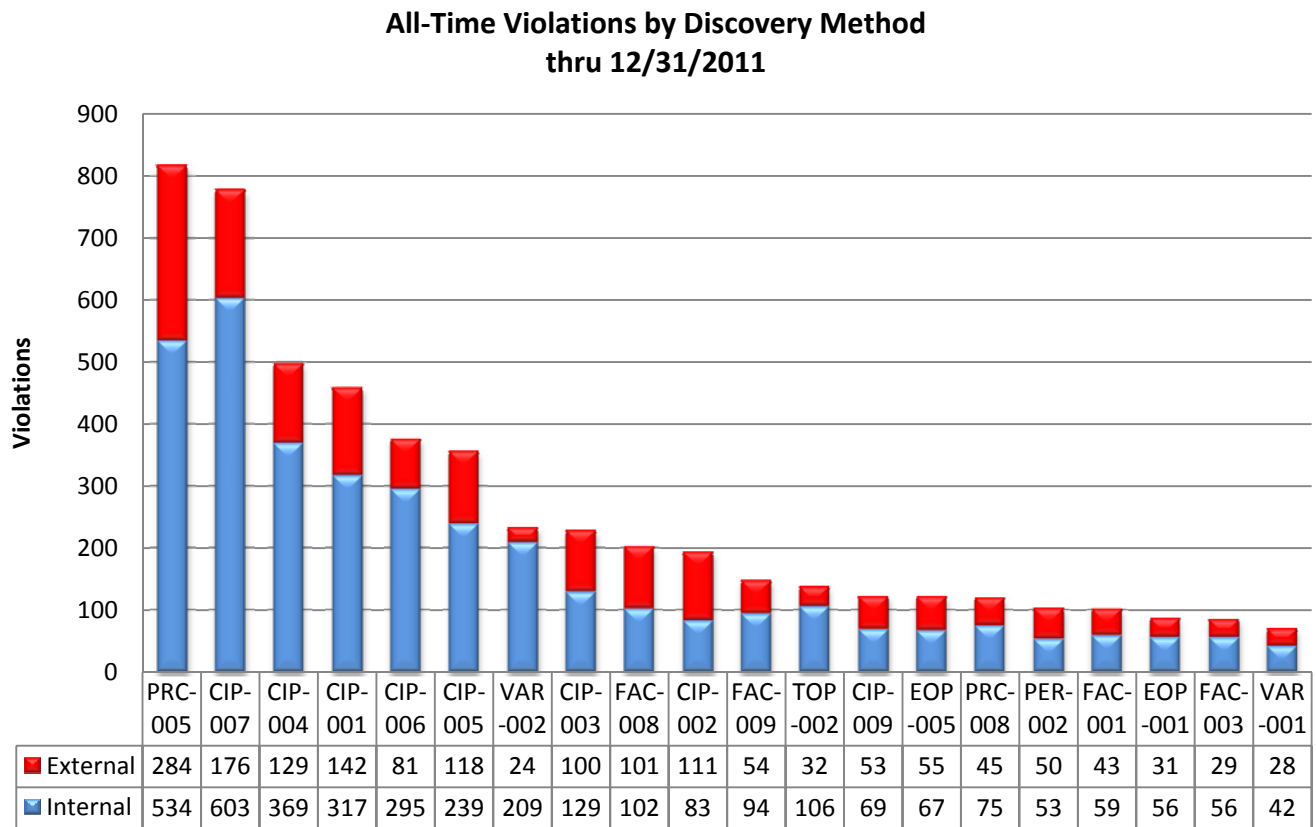


Figure 5: Top 20 Violated NERC Reliability Standards All Time through 2011

2011 Violations by Discovery Method

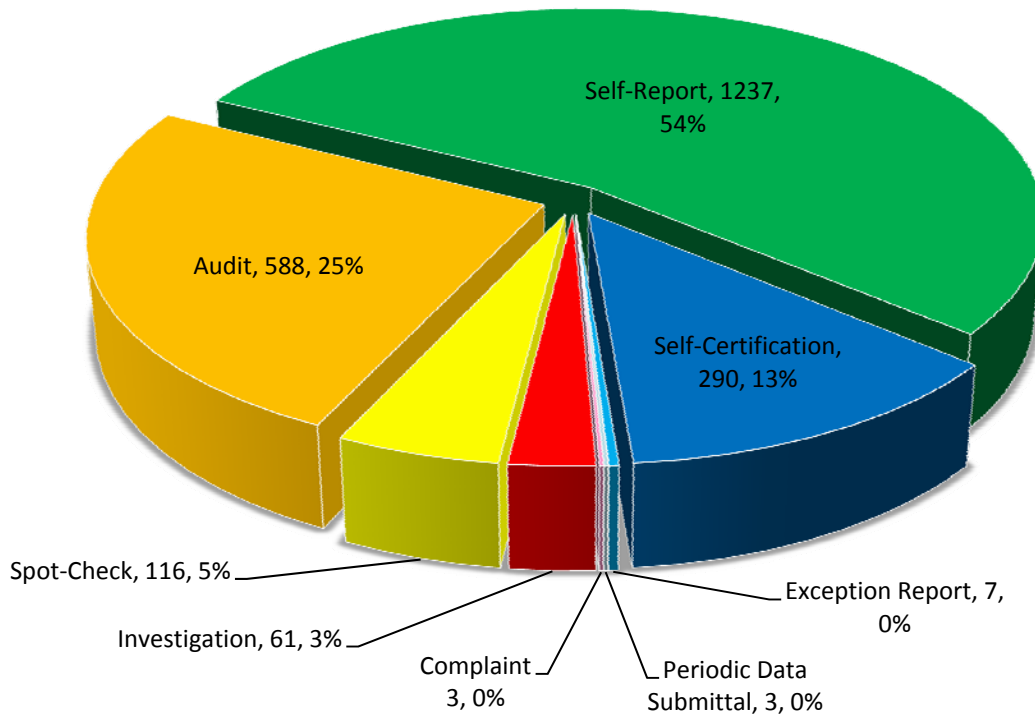


Figure 6: Discovery Methods of the Top 20 Violations of NERC Reliability Standards in 2011

Figure 6 provides a breakdown of the violations in 2011 by way of discovery method. The largest proportion of violations within 2011 was discovered by way of self-reports, which is very positive considering that self-reports reflect an internalized understanding of reliability standards. Self-identified discovery methods, both self-report and self-certification, account for 67% of all violations discovered in 2011. This equates to a 2% increase in self reporting from 2010. The second most frequently occurring discovery method for violations in 2011 was compliance audits at 25%. Externally identified discovery methods account for 33% of all discovered violations in 2011.

Self-identified discovery methods,
both self-report and
self-certification, account for 67% of
all violations discovered in 2011.

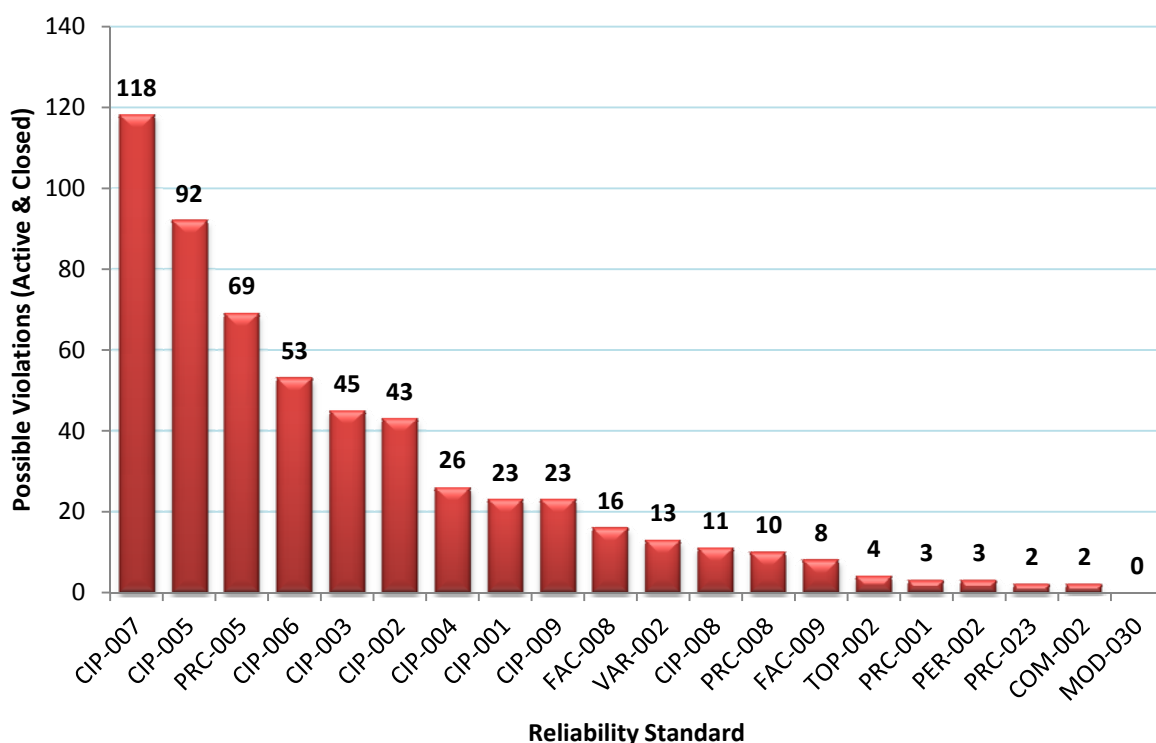


Figure 7: Violations Discovered during an Audit by Standard in 2011

The NERC Reliability Standards that received PVs that were discovered during an audit are graphically depicted in figure 7. As with the most violated standards of all time, CIP-002 through CIP-009 standards are heavily represented, accounting for seven within the top ten.

The following figures 8 and 9 show the breakdown of PVs by way of a registered entity's function. Figure 8 describes this relationship over the year of 2011, whereas; figure 9 describes the data from an all time perspective of 2007 through 2011. Generally speaking, these two sample data sets are extremely similar; indicating that known challenges with standards compliance continue to predictably affect entities with the same BES function. Collectively, the Transmission Operator (TOP) and Transmission Owner (TO) functions outpace all other functions for the most PVs. Generator Operator (GOP) and Generator Owner (GO) collectively follow the transmission functions and also lead the remaining functions. Although not as often as the previously mentioned functions, the Load-Serving Entity (LSE), Balancing Authority (BA), and Transmission Service Provider (TSP) functions consistently draw a significant number of PVs. The remaining nine functions are mildly represented with regards to receiving PVs.

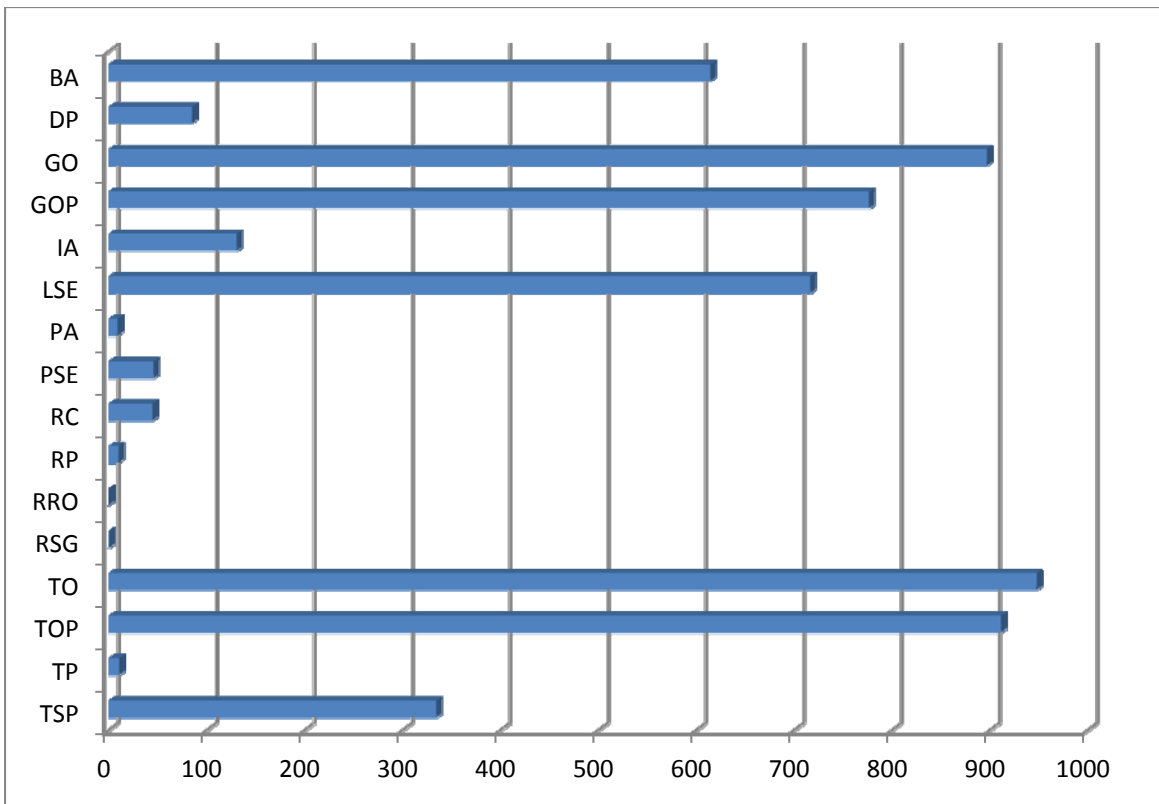


Figure 8: Number of Possible Violations by Function for 2011

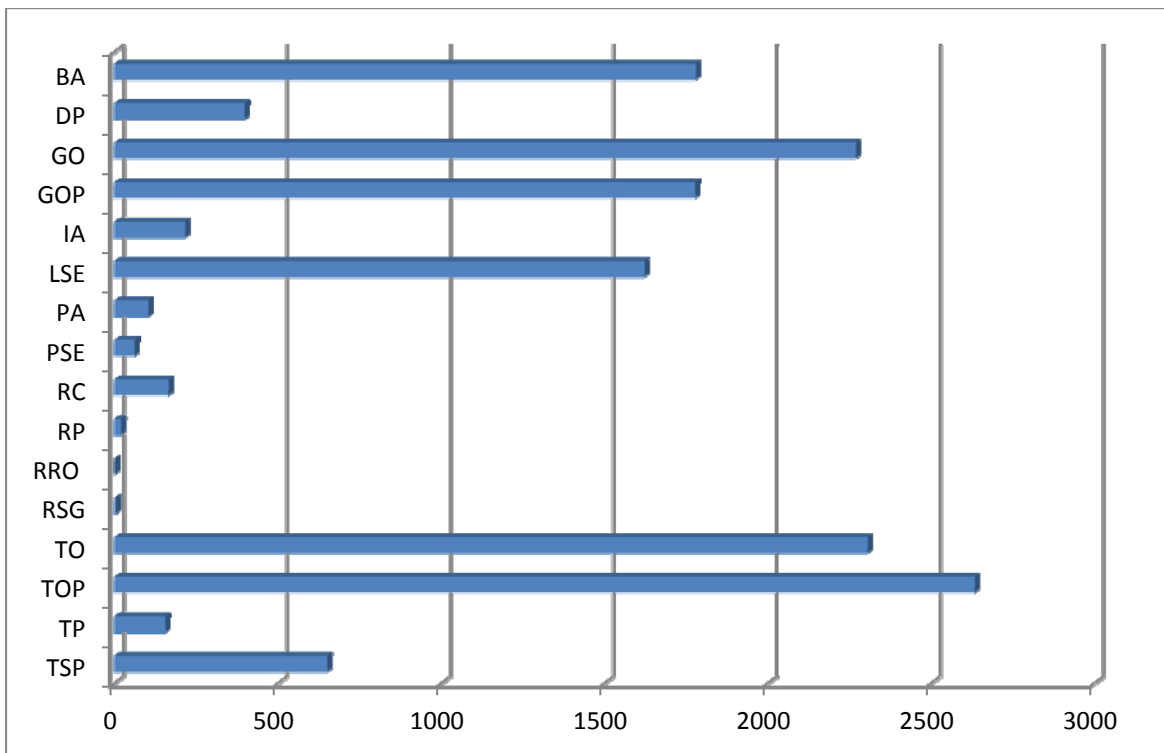


Figure 9: Number of Possible Violations by Function for 2007 through 2011

In an effort to measure and understand the appropriateness of using a risk-based tiered system within the 2011 AML, PV data was balanced against a standard's tier membership. The graphs on the following two pages depict this data across two separate bar charts. Figure 10 shows the number of violations that occurred with a standard that contains any of the 2011 AML Tier 1, 2, or 3 requirements. And conversely, figure 11 depicts the number of violations recorded for a standard that contained no tiered requirement.

Figure 10 shows that seven of the 45 tiered standards had 100 or more Possible Violations. The remaining tiered standards averaged nearly 12 Possible Violations per standard. As for figure 11⁴⁶ and with regards to the 34 non-tiered standards, all but four standards received less than ten PVs, with an average across these standards being three violations. Four non-tiered standards had a number of PVs well above this average: VAR-002 (Generator Operation for Maintaining Network Voltage Schedules) had 95, MOD-030 (Flowgate Methodology) had 19, VAR-501 WECC-1 (Power System Stabilizer) had 12, and BAL-005 (Automatic Generation Control) had 11 violations.

⁴⁶ As of July 2011, WECC standards VAR-STD-002a-1 and VAR-STD-2b-1 were replaced with VAR-002-WECC-1 and VAR-501-WECC-1.

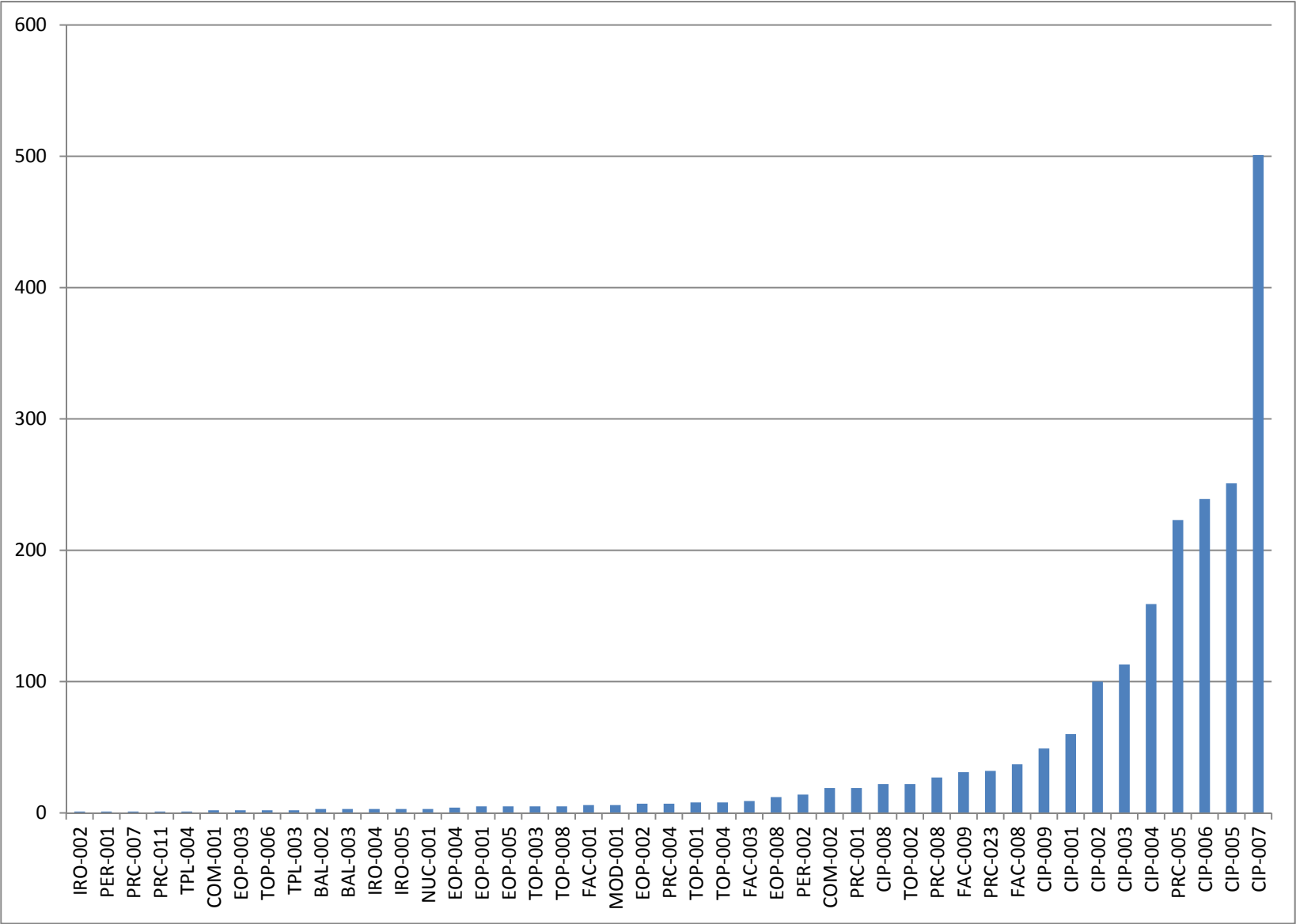


Figure 10: Possible Violations of Tiered Standards for 2011

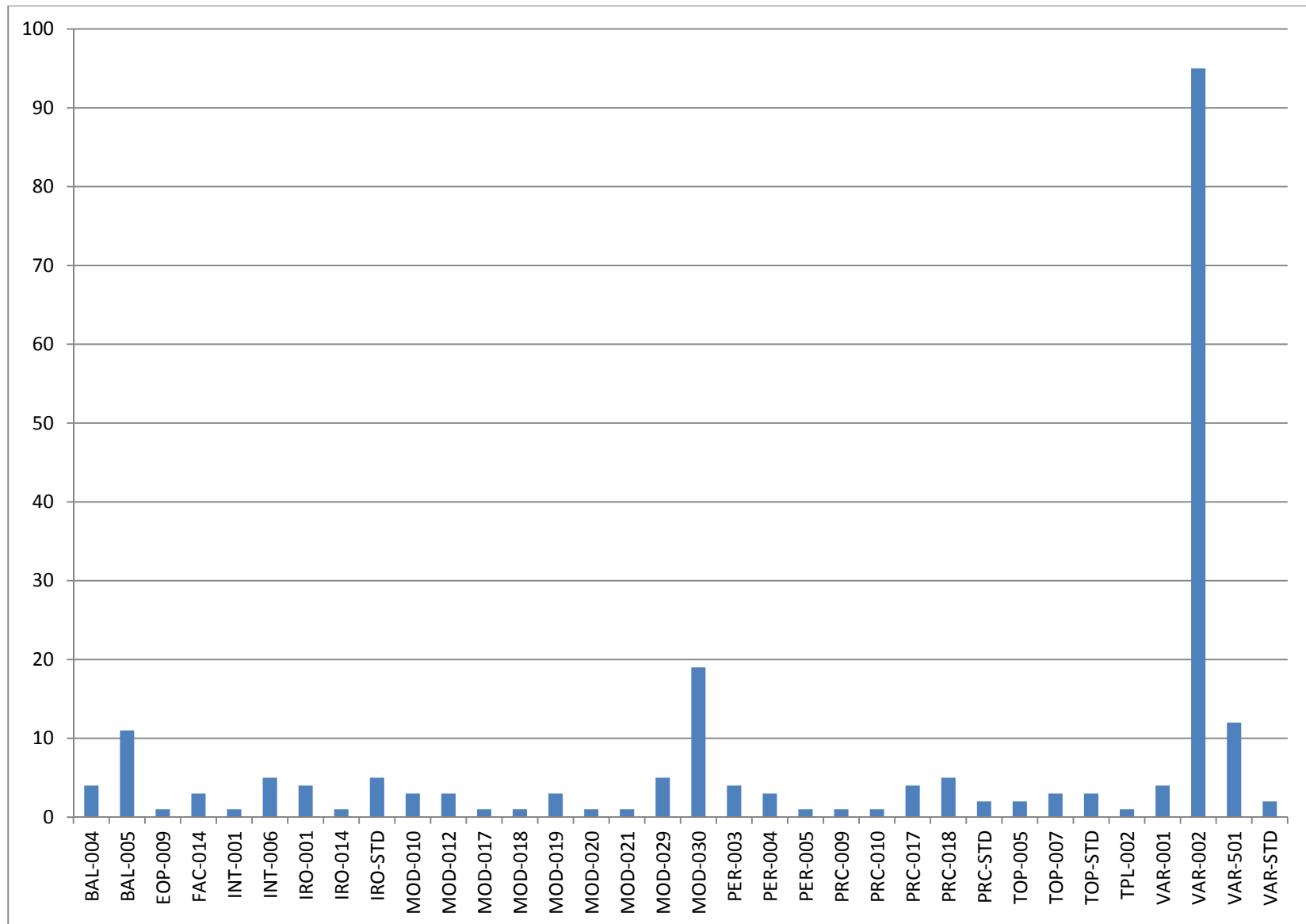


Figure 11: Possible Violations of Non-Tiered Standards for 2011

The below Table 5 and Table 6, identify the standards that have never been violated and the standards that have minimally been violated. This information can be used in the development of the 2013 implementation plan and future similar type risk assessments.

Table 5: Reliability Standards That Have Never Had an Associated Possible Violation			
BAL-502	IRO-008	MOD-008	PRC-003
BAL-STD	IRO-009	MOD-009	PRC-006
EOP-007	IRO-010	MOD-011	PRC-012
FAC-011	IRO-015	MOD-013	PRC-013
FAC-012	IRO-016	MOD-014	PRC-014
FAC-501	MOD-002	MOD-015	PRC-020
INT-007	MOD-003	MOD-016	PRC-022
INT-008	MOD-004	MOD-024	TPL-005
INT-010	MOD-005	MOD-025	TPL-006
IRO-006	MOD-007	PRC-002	

Table 6: Reliability Standards with One to Five Possible Violations 2007 through 2011			
FAC-002	PRC-009	BAL-001	INT-001
INT-005	EOP-009	BAL-006	MOD-018
IRO-002	FAC-013	INT-009	NUC-001
IRO-003	INT-003	MOD-006	MOD-029
MOD-020	IRO-014	MOD-019	
MOD-021	MOD-017	PRC-010	
MOD-028	PRC-016	PRC-015	
PER-005	PRC-021	EOP-006	

Enforcement Processing

Compliance Enforcement continued to improve its efficiency in processing violations of the NERC Reliability Standards in 2011. The utilization of new reporting and filing formats helped facilitate more efficient and effective processing of violations.

The number of active violations increased in 2011. This increase resulted from growth in the average number of new violations per month from 168 in 2010 to an average of 245 violations

per month in 2011. The increase in active violations can be at least partially attributed to the implementation of NERC's CIP standards.

Compliance Enforcement implemented several new processes in 2011 that contributed to increased efficiency. The number of violations filed by NERC increased from 64 per month in 2010 to 141 per month in 2011. When factoring in dismissals, the improvement is even more vivid: in 2010, 90 violations per month were filed with FERC or dismissed; in 2011, 217 violations per month were filed with FERC or dismissed. In six of the last seven months of 2011, NERC processed more violations than it received. These successes owe to increased collaboration with REs increases in the number and expertise of Compliance Enforcement staff and improved enforcement processing tools such as FFT.

Compliance Enforcement used an Administrative Citation Process from January to August of 2011 that included the filing of 285 violations. With the Administrative Citation NOP, numerous lower-risk violations were submitted in a single streamlined NOP, reducing several levels of process and documentation. In September, Compliance Enforcement made its initial CEI filing with FERC that introduced the streamlined Spreadsheet Notice of Penalty (SNOP) and the FFT approaches to address lesser risk to reliability issues. The CEI has received significant support from the REs and the industry. The first four Spreadsheet NOP filings, containing 235 violations, were accepted by FERC with no further review. For the period of September through December 2011, 325 FFTs were filed and accepted through the Commission's March 15, 2012 Order.

For details regarding enforcements processing improvements as part of the CEI please refer to the FFT portion of the Significant 2011 Projects section of this report.

Regional Entities CMEP Activities

Each of the eight REs have been sent a series of questions addressing seven aspects of their experience with implementing the 2011 CMEP. These seven aspects address Compliance Monitoring, Compliance Outreach, Compliance Enforcement, Program Effectiveness, Events Analysis and Compliance Review, RE Metrics, and Projections for the Future. The responses of the REs are summarized in the sections that follow.

Compliance Monitoring

Compliance Monitoring seeks to discover a number of details surrounding the audits performed by the REs. There were 463 compliance audits planned in 2011, as identified by unique NERC Compliance Registry identification numbers. 276 of these audits were for Operations and Planning reliability standards (693 audits) while 217 of these were for CIP reliability standards (CIP audits). Figure 14 below shows the breakdown of these audit efforts by Region. NPCC, RFC, and WECC were successful in completing their planned audits. MRO had one audit with a non-FERC jurisdictional entity that was postponed for one year in order for the registered entity to develop their compliance program in accordance with reliability standards and requirements deemed enforceable by their regulatory body. SERC had one scheduled audit of a Reserve Sharing Group (RSG) that was cancelled based upon NERC approval of a reduction in audit scope. SPP had one audit that was deferred by NERC, one audit that was cancelled due to change of registration, and one audit that was cancelled due to change of registration. TRE had two audits of affiliated entities that were not completed as scheduled, because the two entities sold their assets during 2011 and were deregistered. TRE instead completed CIP and 693 spot checks of these entities. Furthermore, TRE did not complete a scheduled GO/GOP audit due to the entity becoming de-registered.

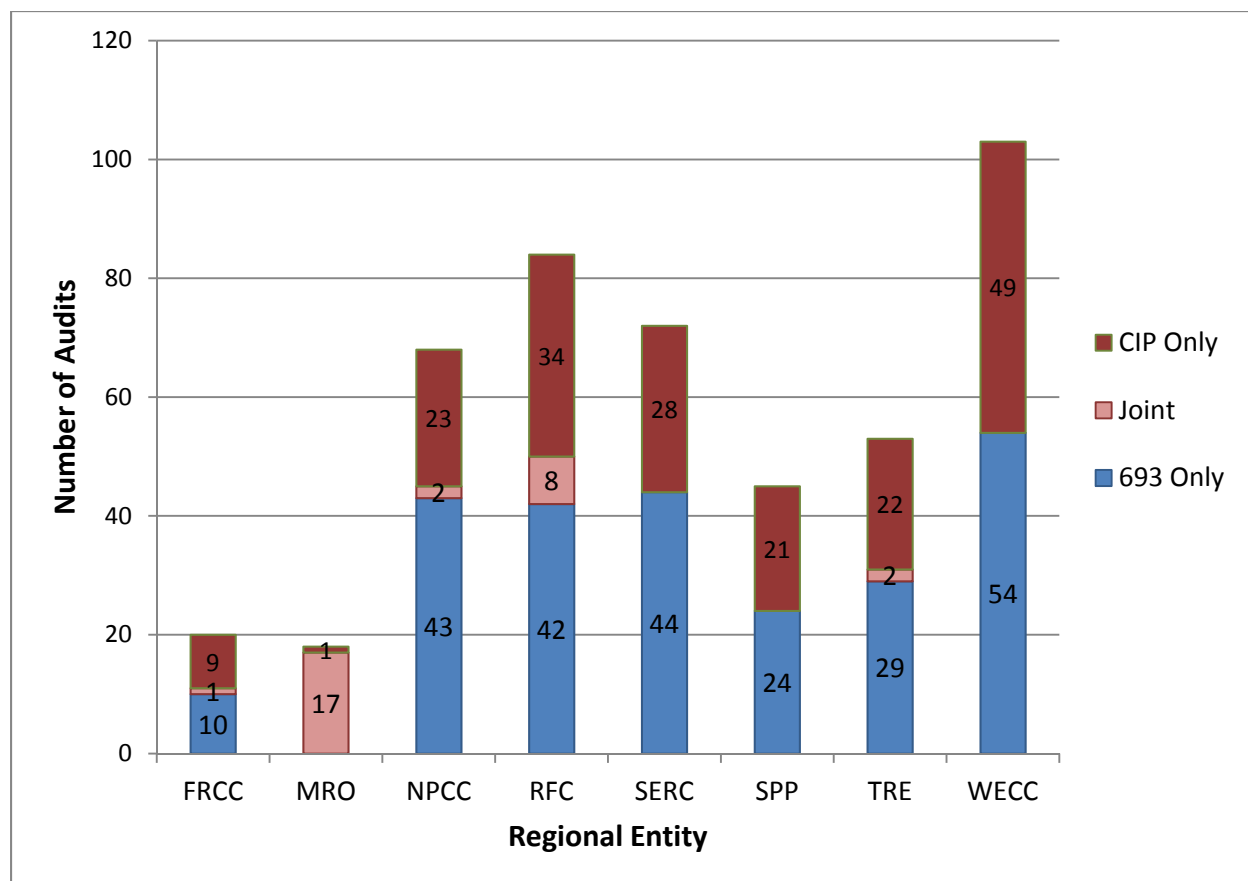


Figure 14: Reported Regional Entity Participation in 693 and CIP Audits in 2011

All of the REs have reported a timely completion of their three year audit cycles in 2011 with one exception. This exception relates to MRO, which, as previously described, had one audit with a non-FERC jurisdictional entity that was postponed for one year in order for the RE to develop their compliance program. This entity previously was audited in 2008 without a MOU in place. As for the six year audit cycles, all REs reported that they were on track for a timely completion in 2013.

With regards to the completion of Regional audit reports, REs have indicated that they have faced challenges in meeting the suggested 60 day timeframe requirement. Personnel resources and time are clearly the limiting factors delaying completion of the reports. That being said, most of the REs note that, when averaged, report completion is within the 60 day requirement. Of interest, one RE noted that a timeframe of 70 days is used. This allows for non-business days and still holds to the 60 day requirement.

Compliance Outreach

Compliance Outreach looks into the REs interactions with registered entities that are taking place in order to provide information and promote transparency about the CMEP process to the registrants. To this end, all of the REs held a number of workshops during 2011 for Operations and Planning and CIP reliability standards. The number of stakeholder participants

for each RE is shown graphically in Figure 15. The total number of workshop participants amounts to 4,365. Of note, WECC accounted for roughly one-third of this total. At least a partial basis for the large number of participants for WECC is due to the fact that WECC holds monthly open WebEx calls with pre-set agendas and time for questions and answers.

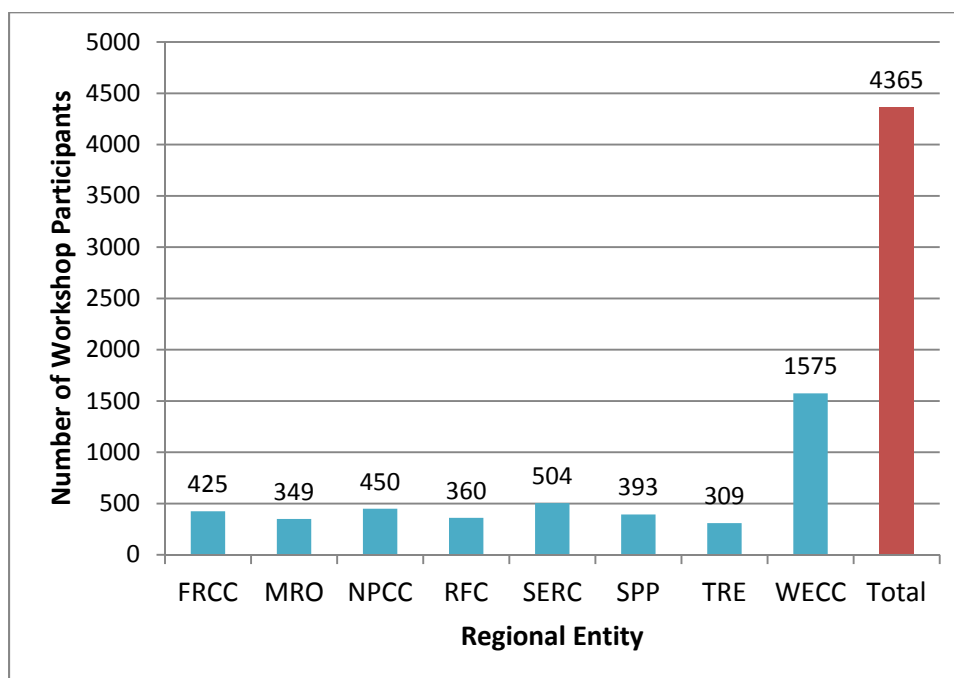


Figure 15: 2011 Workshop Participants by Regional Entity

Throughout the REs, feedback from the workshops has been very positive and participants are requesting that additional topics be covered. To fulfill the desire from the industry for an increased level of compliance information, as well as, to enhance CMEP transparency, many of the REs have provided workshop sessions specifically aimed at requests made by the attendees. Specifically, several REs have led presentations that teach to the application of standards and methods of demonstrating compliance. Small registered entity involvement and attendance in workshops was a priority for two REs. One Region employed mock audits as a training tool in one of the workshops that they conducted.

Compliance Enforcement

Compliance Enforcement looks to improve enforcement processing for the benefit of registered entities, REs, and NERC. The administrative citation process brought efficiency gains to the REs, but not to the extent that was expected. Several REs pointed out that the administrative citation process utilized many time-consuming steps normally required when processing violations, such as the assessment of a violation's scope and its potential risk to BPS reliability. Some REs found value in the use of the spreadsheet for providing violation information, so they have benefited from the expanded use of the spreadsheet with the Spreadsheet NOP.

The FFT process is designed as a tool for the REs to evaluate existing and new violations to determine whether they can be processed and closed without assessment of a penalty. For

minimal risk violations for which assessment of a penalty would provide little reliability or educational value, the REs can take advantage of the FFT process to handle such violations with fewer processes and less documentation. This increased proportionality enables the REs to work more closely with their registered entities on reliability excellence instead of spending significant resources on enforcement. This is a refocusing of ERO resources, not a reduction of resources or a step back from maintaining reliability and accountability.

Many of the challenges for Compliance Enforcement programs across the REs continue to center on staffing shortages and the processing of violations, especially those dealing with CIP standards. To combat staffing shortages, many REs have indicated that a number of positions have been filled with a specific focus on improving violation processing. Also, the REs have brought on cyber security experts in dedicated compliance enforcement roles for the additional workload brought about by CIP. Compliance Enforcement continues to work with the REs on efficient processing of their violations.

Several REs noted and outlined the improvements that their compliance enforcement program underwent in 2011. Maturity of internal processes and development of competent employees directly accounted for the measurable improvements. As an example, RFC reported that outgoing violations being filed with NERC almost tripled (546 in 2011 vs. 171 in 2010), the average number of days for violation disposition decreased by 16% (228 days in 2011 vs. 270 days in 2010), and the average number of labor hours for enforcement processing of violations decreased to 59% (37 hours per violation in 2011 v. 99 hours per violation in 2010).

Program Effectiveness

Program Effectiveness has the REs document the positive aspects encountered throughout the implementation of the 2011 CMEP as well as those areas needing improvement. Beginning with the areas needing improvement, all of the REs noted that the monitoring and enforcement of CIP standards continue to be a significant technical and logistical challenge. Additionally, the processing and management of CIP TFEs has only added to this challenge of processing CIP enforcement actions. Maintaining and increasing the staffing of qualified individuals throughout all areas within the CMEP has been difficult, not only at the Regional level but within the registered entities themselves. For example, TRE has noted that some smaller entities retain outside consultants to act as the primary compliance contact, which tends to adversely affect the entities' role in compliance monitoring or enforcement activities.

The positive aspects of the 2011 CMEP are many. As with last year, nearly all REs reported that there has been considerable growth in the number of self-identified violations, especially through self-reports and self-certifications. This increase in self-identified violations has been especially noted for those entities with comprehensive internal compliance programs that proactively assess compliance. Several REs have reported that improved data transmission processes between the audit team and registered entity have resulted in a significant reduction to the man-hours required to complete an audit. The use of secure web portals has dramatically lowered the time CIP auditor are required to be on-site and simple tools such as color coding documents or generally organizing evidence for audit review have gone a long way in making the most of audit time. Concurrently, REs have had their auditors completing due

diligence efforts more thoroughly during the pre-audit phases, likewise resulting in lowering audit time man-hours. More and more compliance programs are being projected within the policies and procedures that the registered entities are using on a daily basis, leading to, as MRO phrases it, operationalized compliance. A couple of the REs also noted that they have taken steps to more closely align their compliance monitoring and enforcement processes and documentation with NERC. SERC staff achieved a significant milestone by being the first RE to synch its compliance tracking database with NERC's database, eliminating the burdensome workbooks previously used to track status of compliance violations. The use and sharing of auditor tools, such as an evidence sampling methodology and evidence tracking sheets, has continued to help enhance consistency and efficiency across the REs. The initiation of the EA field trial has proven to be a valuable tool in terms of discovering and implementing actions for the enhancement of BPS reliability.

One of the particularly noteworthy aspects of the 2011 CMEP was the implementation of the new EA process, especially in light of the Southwest Winter Event. Being the first RE to have a Category 4 event at the time that the EA process was in evolution was quite time consuming for TRE and its registered entities. The coordination between NERC, FERC, and the Public Utility Commission of Texas was sometimes difficult to manage, causing extra burdens upon TRE and the registered entities. Most of the issues were resolved and much was learned during the analysis of the system event. Having this process completed, provides transparency and consistency for future event analysis.

Events Analysis and Compliance Review

To support a strong culture of compliance, registered entities are expected to perform a compliance analysis and to develop a compliance self-assessment report proportional to the significance of the event or risk to the BPS for categorized events in which there could be a gap between actual system or human performance and the requirements of NERC or Regional reliability standards. Registered entities are encouraged to submit a compliance self-assessment report to the Regional Entity compliance liaison proportional to the significance of the event or risk to the BPS for categorized events. This report should encompass a sufficiency review, proportional to the event's significance, of applicable standards associated with the event.

Registered entities that make a good faith effort to self-identify and self-disclose possible violations stemming from their EA will be afforded consideration in any enforcement action in accordance with NERC's Sanction Guidelines. If further analysis by the RE or NERC reveals other PVs, the registered entity's participation and cooperation will be noted and considered.

For this reason, it is recommended that registered entities establish a liaison between their internal event analysis and compliance functions. This will provide a clearer understanding and a more efficient transfer of information from both an operational and a compliance standpoint, and it will facilitate a thorough standards review by the registered entity.

Figure 16 illustrates the number of events that have been analyzed per RE using this self assessment process.

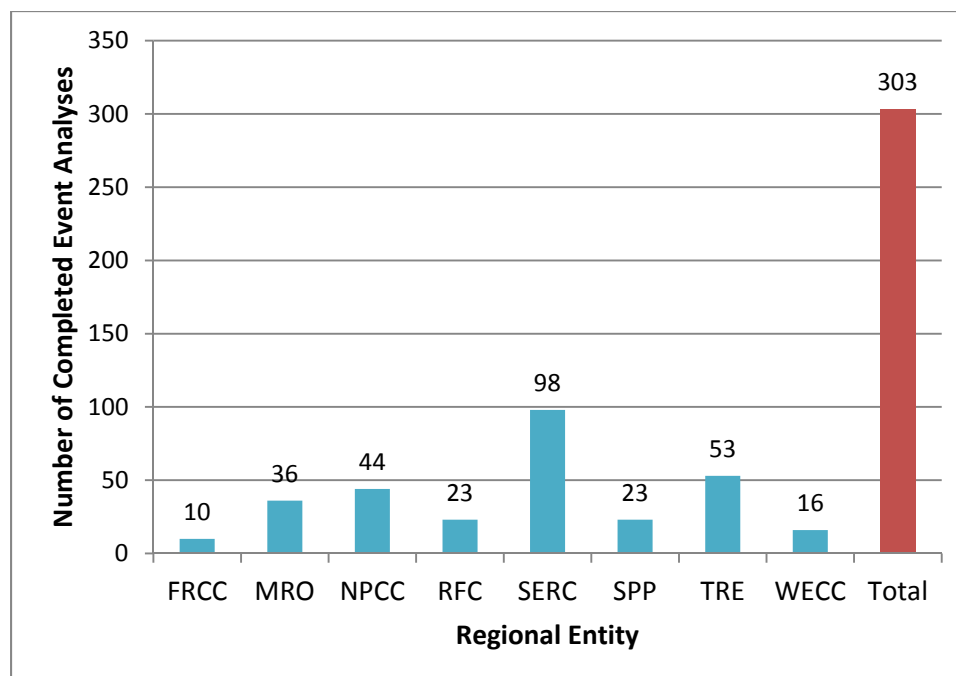


Figure 16: 2011 Completed Event Analyses by Regional Entity

Regional Entity Metrics

The RE Metrics portion of the questionnaire asked the REs to describe, submit, and draw conclusions from any metrics that are being used to measure their CMEP performance. Each RE reported that the use of metrics has been very valuable. Tracking of audits, spot checks, Notice of Violations, mitigation plans, budgeting constraints, and resource planning are common processes being monitored. Additionally, it was noted that the metrics being used are the first steps towards a series of possible metrics that could be used to track performance of stakeholders, as well as, provide a means to measure performance relative to other REs.

Adoption of specific CMEP performance metrics and goals is proving to be useful in helping focus RE staff on specific performance targets and informing management of potential resource constraints, as the metrics reveal how efficiently the REs are processing audit reports, and subsequently notifying NERC and the registered entity of compliance audit findings. For example, metrics are being used to measure the process time undertaken when enforcement is notified of a PV, until the time that enforcement notifies the registered entity of the alleged violation. Metrics such as these are helping the REs focus on key objectives in the compliance monitoring and enforcement areas and sub-sequentially helping add focus to these areas.

Moving forward, the ERO Compliance and Enforcement Management Group (ECEMG) has taken on the project of providing a means of metric consistency between the Regional Entities.

Projections for the Future

Projections for the Future asks the REs about the improvements they would like to see instituted for progressing the CMEP in future years. The most active responses centered on the NERC AML, CEI, and risk-based auditing program.

Most REs found that the newly instituted tiered approach to auditing was beneficial, in that, the process undoubtedly identifies those standards and requirements that have a direct impact on the reliability of the BPS. That being said, each RE was able to specifically identify areas where the tiered system could be improved. Most often mentioned was including, in the same tier, all sub-requirements of any single requirement. This would lead to a more straightforward grouping and a less confusing audit approach, especially when CIP standards are being audited. Several REs commented that a review of the tiered approach as a whole should be conducted by NERC with the goal of performing a trend analysis. This could reveal if any patterns exist that might warrant a tier 2 or tier 3 requirements becoming a tier 1 requirement. Mentioned several times from RE to RE was the idea of removing the monitoring of PSE-only entities via audit or spot check as these are limited critical standards, and the value of the active monitoring may not justify its the cost. An alternate approach to PSE-only monitoring such as self-certification or targeted spot check may be sufficient to ensure compliance. On a more negative note, one RE recommended that in 2013, the AML should be developed without the tiered approach due to registered entities being confused by its implementation because of the non-uniform process being employed across the REs. Instead, NERC should identify those global risks to the BPS which are important to be monitored for 2013 based upon its perspective; using the existing reliability statics or criteria or both developed between NERC and the REs. Using this type of process, the list could more directly employ the risk-based audit approach. All standards are always subject to inclusion into a scope of an audit based upon further focused assessment of the entity by the RE. REs also requested that the AML be reviewed to avoid changes which have caused retractions and re-notifications to entities that have already been notified of audits or spot checks; thereby avoiding logistical challenges that arise when changes in audit scope occur.

The REs are supportive of the CEI and believe that being able to utilize the appropriate discretion relation to reliability risk is a step in the right direction. To further develop the process, RE workshops for the industry as a whole need to focus more on reliability risk and less on compliance risk. Moreover, registered entities need to be educated on the context of risk that needs to be addressed; especially in the enforcement process. To increase all registered entities' understanding, it would be useful if NERC were to provide training of risk assessment as used in the determination of FFT treatment or the evaluation of appropriate Penalties in NOP. As an incentive, NERC could provide a policy that an entity's participation in the EA process and the use industry compliance-self-assessment and standards-review be viewed as strong indicator of that entity's compliance and reliability culture, and therefore, that entity be rewarded by a credit based on a specific formula should a compliance violation be discovered. With regards to CEI logistics, the REs are seeking improvements in the transfer, storage, and reporting of data, as well as, a means to provide quick and ready access to comparative statistics such as violations, mitigation plans, dismissals, and disposition between themselves.

Most REs have developed a risk-based methodology to be used for conducting an assessment of each registered entity scheduled to be audited. The intent of these assessments is to identify unique entity risks which may have an impact to the BES, and as a result, select additional standards which will be recommended for implementation of the monitoring process. This approach best focuses audit team resources and, in some cases, can reduce the monitoring requirements of an entity. In their risk-based approach, ReliabilityFirst in 2012 will increase the

scope of any audit or decide to do a spot check if it believes that additional risks are present in the entities performance during the audit. Auditors are being made aware of the guidance coming out of NERC and will be given additional training on risk and performance based auditing as it evolves. At FRCC, they will be utilizing a draft registered entity risk-based assessment template for identifying all pertinent operating data related to a registered entity, including violation history data, to assist the compliance staff in determining the risk to the BES a particular registered entity may have. They will then be working with NERC to develop the registered entity risk-based assessment template. NPCC reports that they will evaluate each entity and the potential risk-based on entity's registered functions, risk to the BES, audit history, self reports, and spot check history of the entity. To approach the challenges of a risk-based program, MRO has sought out auditors and personnel who are credentialed, trained, and experienced. Furthermore, they recommend that NERC administer a program which develops similarly skilled personnel throughout all REs.

Significant 2011 Projects

Defining the Bulk Electric System

On November 18, 2010, FERC issued an Order (Order No. 743) directing NERC to revise the definition of the BES using the reliability standards development process and address the Commission's technical concerns as identified in that Order. NERC was also directed to develop and submit an implementation plan or plans for the revised BES Definition. FERC established a January 25, 2012 deadline for filing the revised BES Definition, the implementation plan, and the proposed BES Exception Procedure with the Commission. A revised BES definition and implementation plan was developed and successfully balloted through the reliability standards development process. Modifications to NERC's ROP to address the BES Exception Procedure were undertaken as well. Those modifications, along with the revised BES definition and implementation plan, were adopted by the BOT on January 18, 2012. The proposed revisions remain pending before the commission.

The proposed revised BES Definition eliminates the phrase "as defined by the Regional Reliability Organization" contained in the current definition, thereby eliminating the explicit basis for RE discretion that was one of the Commission's primary concerns in Order Nos. 743 and 743-A. It also provides a default threshold of Transmission Elements operated, and Real Power and Reactive Power resources connected at, 100 kV or higher. That "bright line" is augmented by a list of five categories of facilities that are included in the BES and a list of four categories of facilities that are excluded from the BES. The listed Inclusions and Exclusions address and provide clarity both to types of facilities that were the subject of FERC's technical concerns in Order No. 743 and to types of facilities that have been problematic previously when determining whether or not they are included in the BES.

There are three sets of proposed modifications to the NERC ROP that were made in support of this effort – modification of Section 509, Section 1703, and Appendix 5C. Section 509 states that an Element is considered to be (or not to be) part of the BES by applying the BES Definition, and that Appendix 5C sets forth the procedures by which an entity may request a determination that an Element that falls within the BES Definition should be exempted from being considered part of the BES, as well as how an entity may request that an Element that falls outside the BES definition should be considered a part of the BES. Appendix 5C sets forth the detailed procedural steps for submission of an exception request by an entity, consideration of the Exception Request by the applicable RE and NERC, and the decision by NERC to approve or disapprove the exception request. Section 1703 sets forth the steps by which an entity may ask the BOTCC to review the NERC decision to approve or disapprove an exception request.

In support of these changes, a form for the submission of Detailed Information to Support an exception request was developed. This form provides separate sets of questions applicable to Transmission Elements, and to generation resources, for which an exception is being requested. This information is used by the RE and NERC in evaluating whether the elements that are the subject of an exception request are necessary for reliably operating the interconnected transmission network. The entity requesting the exception remains responsible to present sufficient information and argument to justify it.

It is proposed that the revised BES Definition be effective on the first day of the second calendar quarter after receiving applicable regulatory approval, or, in those jurisdictions where no regulatory approval is required, the revised BES Definition should go into effect on the first day of the second calendar quarter after its adoption by the BOT. However, recognizing that there will be changes regarding what facilities fall within the scope of NERC standards based on this new definition, it is proposed that that compliance obligations for all elements newly identified to be included in the BES based on the revised BES Definition should begin 24 months after the applicable effective date of the revised BES Definition.

This work has only recently been filed with regulators, and at the time of the writing of this document, it is unclear when these changes will go into effect. As such, it is unlikely that there will be any impact to Compliance and Enforcement in 2012, but it is important to note that there is a potential for changes in the future, which may necessitate additional staff or other resources.

Find, Fix, and Track

FFT Filing

NERC and the REs have continued to seek ways to improve its processes and the quality of reliability standards. NERC, the REs, FERC, and the industry have discussed significant ways to retool efficiency efforts through multiple technical conferences. A key outcome was the recognition that compliance matters should be treated differently based on the level of risk posed to the reliability of the BPS.

NERC's new CEI is designed to handle issues more efficiently, focus on issues posing a higher risk to reliability, streamline administrative paperwork, and continue to encourage self-reporting and mitigation.

NERC is not looking to reduce the number of compliance items identified with this new initiative, but is rather looking to treat matters differently based upon the risk associated with them. By identifying, mitigating and quickly resolving issues that pose a minimal risk, more resources can be focused on violations that pose a more serious risk to reliability.

The CEI is being launched in accordance with NERC's Rules of Procedure. The new initiative is not about whether issues will be addressed. Rather, it is about how they are addressed.

Following NERC's filing⁴⁷ of the CEI on September 30, 2011 and FERC's Order⁴⁸ accepting the process on March 15, 2012, there are three enforcement tracks: Dismissal; FFT; and NOP. Dismissals occur where there are no violations, when the entity is not registered for and/or

⁴⁷ See North American Electric Reliability Corporation, "Petition Requesting Approval of New Enforcement Mechanisms and Submittal of Initial Informational Filing Regarding NERC's Efforts to Refocus Implementation of its Compliance Monitoring and Enforcement Program": http://www.nerc.com/files/FinalFiled_CEI_Document_20110930.pdf

⁴⁸ See Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing, 138 FERC ¶ 61,193 (2012) at: http://www.nerc.com/files/OrderConditionallyAcceptingNewEnforcementMechFiling_031512.pdf

subject to a particular requirement, or where there are duplicate entries of issues. No changes are being made with respect to dismissals.

The FFT is the new portion of the compliance initiative. This process will apply when a PV poses a minimal risk to BPS reliability. All matters identified via FFT or NOP must be fixed; the registered entity must provide a statement of completion certified by an officer of the company and completion of mitigation activities is subject to verification by the RE as part of an audit, spot check or random sampling. The issue must be fixed prior to inclusion in a report to FERC. A PV processed through FFT becomes a remediated issue once included in an FFT informational filing and such filing concludes processing of that matter by REs and NERC. No penalties or sanctions will be applied to FFT issues. These remediated issues will be included as part of a registered entity's compliance history and will be taken into account in future actions as appropriate. Mitigation activities must be described in the FFT spreadsheet; however, a formal mitigation plan will not be required.

For those matters that pose a more serious risk to reliability of the BPS, NOPs will be filed. They may be filed either in a spreadsheet format or a full NOP format.

REs will review current cases and determine which disposition approach will be used based on the issue. Training of compliance and enforcement staff will take place as part of the implementation of the FFT process.

Approximately 60 percent of violations are a result of four compliance monitoring methods (self-report, self-certification, data-submittal and exception-reporting) that provide self-identified possible violation reporting by a registered entity. NERC encourages registered entities to include a full factual description of the issue, detailed information regarding mitigation activities, identification of the potential and actual risk posed as well as mitigating factors in effect while a PV is awaiting a determination of the appropriate processing track. This process will help illustrate that the registered entity understands the full scope of the violation and has taken actions to correct it and prevent recurrence.

NERC will continue to compile trend data and keep historical records on registered entities, which will allow NERC to target areas for increased education as needed. Registered entities are expected to provide information that is sufficient, complete and validated to support the issues identified for FFT or NOP treatment.

The CEI, featuring the FFT approach to minimal risk remediated issues, is a paradigm shift in how issues are processed, not whether they are addressed. In all cases, they must be found, fixed and tracked. The CEI reflects a risk-based approach that acknowledges all PVs are not equal and should not be treated as such. By focusing resources on violations that have a serious risk to the reliability of the BPS, NERC is able to better fulfill its mission as the ERO.

FFT Implementation

During the initial phase of FFT implementation, auditors are able to recommend FFT treatment of certain audit findings, but the decision to afford FFT treatment to a specific issue resides with the RE enforcement staff. The next phase of the CEI, currently targeted for 2013, will vest the

decision of processing a violation through the FFT process with the CEA compliance staff as well as enforcement staff. NERC will be providing a series of webinars and workshops to guide compliance and enforcement staff at all levels on the application of FFT to PVs.

NERC also has posted information regarding the CEI implementation on its website. This information includes guidance to registered entities on information to be included in self-reports, particularly with respect to the underlying factual situation, the assessment of the risk to the reliability of the BPS and mitigating activities to correct and prevent PVs. NERC will continue to hold webinars and workshops with the industry to enhance understanding of FFT and the ERO's enforcement efforts. These webinars and workshops will focus on case studies based on the FFT informational filings to date.

In May of 2012, NERC will file with FERC a six-month status update on CEI implementation. In that filing, NERC will describe the experience gained and the results from implementation of the CEI to date. In a concurrent compliance filing, NERC will respond to specified compliance requirements outlined in the March 15th CEI order. Specifically, the six-month report will address and provide context for the CEI processing statistics, discuss the benefits obtained from the program from a broad perspective (NERC, RE and industry) and discuss implementation challenge and how NERC is addressing them. In preparation of this filing, NERC will be working with the REs to ensure their input is incorporated into the filing. NERC has also distributed a survey to solicit information from the registered entities regarding their experience with the implementation of the CEI to date that will also inform the content of the six-month update to FERC.

With additional efficiencies attained with the implementation of the FFT and spreadsheet NOP approach, NERC has been able to process a significant number of cases since September 2011. In the six-month period from September 2011 to the end of February 2012, as reflected in Figure 2, NERC filed 921 total violations, or on average 154 violations filed per month. Of the 921 violations, 428 were FFTs, representing an average filing rate of 71 FFTs per month. Over the past year, the ERO's caseload of active violations expanded from 3260 in February 2011 to 3611 in February 2012. The rate of new violations coming into the case load has increased dramatically from an average of 196 violations per month in February 2011 to an average of 267 violations per month in February 2012. The increase in caseload is primarily attributable to the large number of violations of CIP Standards that have been and will be entering the system.

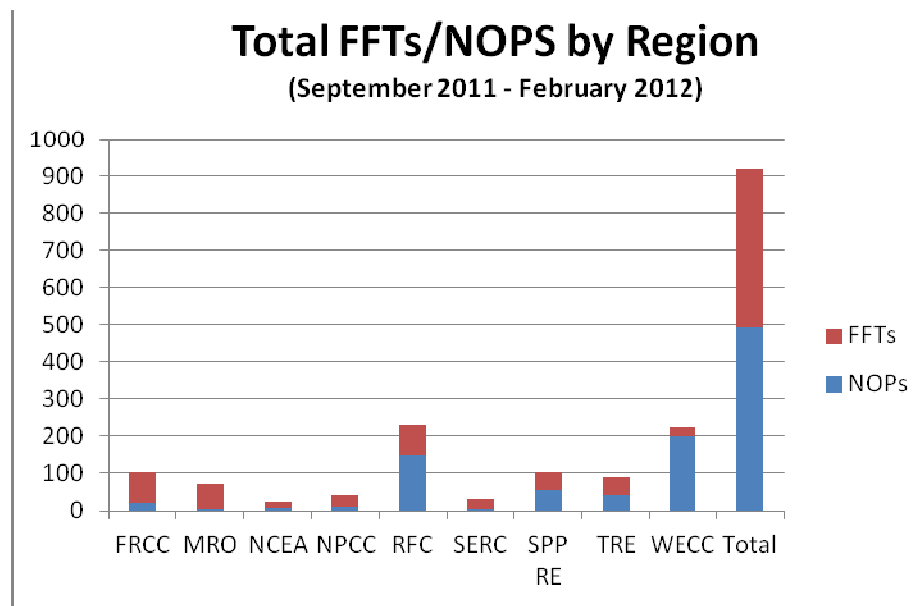


Figure 17: Total FFTs/NOPS by Region

The average monthly processing rate over the last year is 233 violations per month and includes both violations that are filed or dismissed. Figure 18 compares the number of incoming violations each month to the number of violations filed or dismissed. There have been more violations processed than submitted in seven of the last nine months. This is very encouraging and is primarily a result of the new compliance initiative introduced in September 2011.

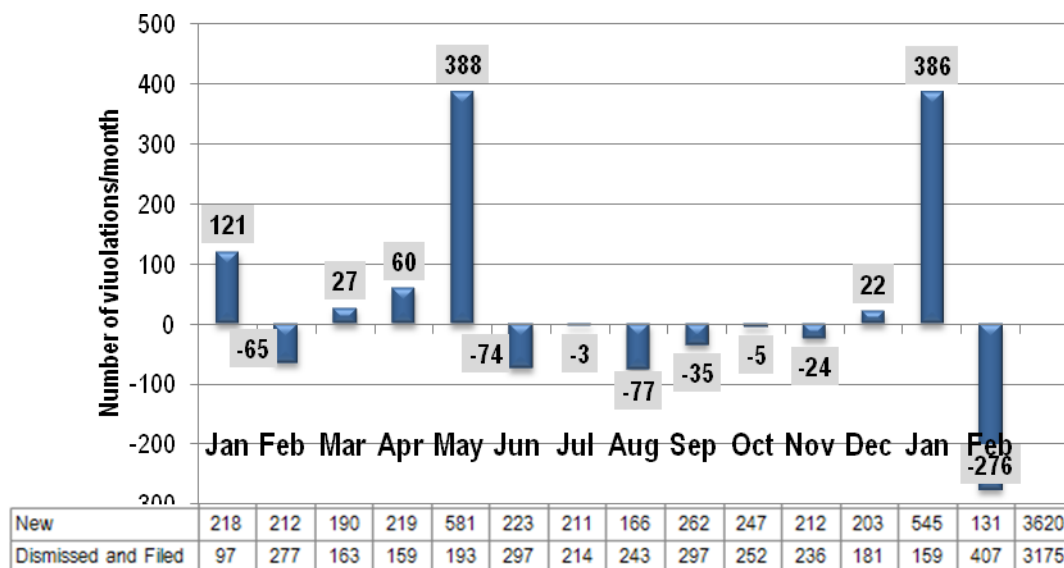


Figure 18: 2011 Violation Process Rate

Registered Entity Assessment

In 2011, NERC and the REs began work on a registered entity Assessment template. This assessment is being developed to establish a consistent basis for appropriately scoping compliance monitoring, to provide an opportunity for REs to work with entities on reliability

efforts and for registered entities to showcase their reliability efforts. Additionally, as a registered entity's Internal Compliance Program will be included in the assessment, the assessment may provide opportunities to identify and share strong Internal Compliance Program models.

The work that was conducted on the registered entity Assessments in 2011 generated significant discussion about what elements should be included in the registered entity assessment template. As a result, the ERO decided to provide more time to develop a template that would be widely accepted as an accurate representation of the entity's profile.

Therefore, in 2012 the ERO is looking to build a registered entity assessment template with direct input from the industry. The first half of 2012 will be dedicated to gathering information from the industry to create a template by the end of the year that will be phased-in through 2013.

Human Performance

NERC has initiated a human performance program, to not only allow a more thorough analysis of the events on the BPS, but also to create a proactive focus on reducing human error and those precursory factors that allow human error to impact system reliability. The transfer of these important reliability messages requires a variety of instruments that can advise practices and training, particularly those that can affect the reliability of the BPS. Sharing across the North American industry allows expertise and experience to strengthen the grid as a whole, making everyone more successful in meeting reliability objectives. The techniques and procedures that NERC is using to propagate this initiative include conferences, workshops, webinars, and publications with facilitated active sharing among NERC and its stakeholders. A purposefully designed NERC sponsored Human Performance Conference is being planned for 2012 to address challenges related to human performance on the reliability of the BPS.

While human error is cited for a large part of the contributing causes for events on the BPS, the RRM is partnering with industry in the EA process and has initiated a new trending analysis system to assimilate the information received in entity reports. The process will aid in developing corresponding corrective action plans to address the causes of an event or failure. These corrective action plans will help to prevent reoccurrence of these events by creating the databases needed to apply the principles of effective risk management. After an investigation, analysis, or determination of causal factors of any event, RRM studies the event or occurrence, often leading to the identification of root causes and causal factors that could drive larger events on the BPS. These processes are applied to all levels of the ERO enterprise, including NERC, the REs, and industry participants that conduct event analysis and are involved in corrective action programs when a cause analysis is required. This process is designed to be a companion process to the ERO EA Process Manual. It is designed to assist those responsible for labeling and trending the causal factors and latent deficiencies leading to BPS events or failures.

CAN Revision Process

Several CANs were in process at the time the NERC BOT instructed the NERC CAN team to revise all existing CANs in August 2011. Those CANs were re-initiated upon finalization of all existing CANs being rewritten and some were still in process at the end of 2011.

The CAN process was revised to illustrate that a CAN provides instructions to CEAs regarding the boundaries within which to assess compliance with standards and requirements. The process also states that a CAN cannot expand a standard and cannot add new requirements.

The CAN process was also revised to provide more opportunities for industry feedback and prioritization. The initial comment period for the revised CAN process was posted on the NERC web site, and industry provided feedback to improve the process. The feedback included requests for more detail on the CAN development process and to vet issues among the NERC executives from each division. Another request from industry stakeholders was to post all industry comments for transparency purposes. Other industry members recommended that NERC provide a method to inform Standards Drafting Teams (SDT) of issues in the CAN. In response, NERC provided the Standards Suggestion Form on the NERC web site. The NERC CAN team implemented the above recommendations and welcomes all feedback to continue improving the CAN process.

The NERC BOT recommended that NERC include a high-level review mechanism in the case that registered entity disagrees with the compliance guidance of a CAN. A review process was created whereby a registered entity or its representatives may submit technical evidence to have a CAN changed or removed. Another option is for the entity to propose a change to the standard through a request for a formal interpretation or a Standard Authorization Request (SAR). The entity may also request a higher-level review of the CAN.

The first review is by NERC's Chief Executive Officer, and the second level of review is by the BOTCC. Also, in accordance with the NERC ROP, a registered entity may contest a violation that was assessed due to the application of a CAN.

NERC is committed to continuing and further developing the CAN program in 2012.

Rated System Path Methodology – MOD-029

MOD-029-1a became effective on April 1, 2011. FERC Order No. 729⁴⁹ has mandated that the MOD reliability standards be audited by the ERO⁵⁰ compliance enforcement authority. The MOD reliability standards have been incorporated into the ERO's CMEP Implementation Plan as of June 1, 2011.⁵¹

⁴⁹ See Mandatory Reliability Standards for the Calculation of Available Transfer Capability, Capacity Benefit Margins, Transmission Reliability Margins, Total Transfer Capability, and Existing Transmission Commitments and Mandatory Reliability Standards for the Bulk-Power System, 129 FERC ¶ 61,155 at P 106 (2009) (Order No. 729) (The Commission hereby adopts the NOPR proposal to direct the ERO to conduct an audit of the various implementation documents developed by transmission service providers to confirm that the complete available transfer capability methodologies reflected therein are sufficiently transparent to allow the Commission and others to replicate and verify those calculations.).

⁵⁰ Id. at P 131 (Upon further consideration, the Commission hereby directs the ERO to conduct these audits in the course of its periodic, three-year audits of users, owners and operators of the Bulk-Power System. The ERO shall begin this audit process 60 days after the implementation of these Reliability Standards.).

⁵¹ The other MOD Reliability Standards, MOD-001-1a, MOD-004-1, MOD-008-1, MOD-028-1, and MOD-030-2 also became effective on April 1, 2011.

Prior to MOD-029-1a becoming effective, a number of registered entities within the Western Interconnection (the “WestConnect Utilities”) submitted to NERC and WECC on February 24, 2011 a request for extension of time to comply with reliability standard MOD-029-1a. NERC granted an extension⁵² of time for all entities subject to MOD-029-1a Requirement (R) 2.1. The basis for this extension was that the methodology contained within MOD-029-1a would, in certain cases, lead to Total Transfer Capability (TTC) and Available Transfer Capability (ATC) values significantly lower than those determined by registered entities under prior TTC calculation methodologies. MOD-029-1a Requirement 2.1 requires the use of power flow simulations to determine TTC:

R2.1. Except where otherwise specified within MOD-029-1a, adjust base case generation and Load levels within the updated power flow model to determine the TTC (maximum flow or reliability limit) that can be simulated on the ATC Path while at the same time satisfying all planning criteria contingencies as follows:

When a power flow simulation identifies a limiting piece of equipment that restricts the amount of flow on a path, that path is considered “Reliability Limited” and the TTC is set based on this limit. When a power flow simulation cannot sufficiently load the transmission path such that a reliability limit is encountered, the path is referred to as being “Flow Limited.” Based upon the language of R2.1, the TTC should be equivalent to either the reliability limit or the flow limit for a path. The complication comes from situations in which the flow limit of a path artificially constrains a path’s TTC below previously utilized levels for which registered entities have demonstrated reliable operations.

To account for this potential issue, NERC has delayed the implementation of requirement MOD-029-1a R2.1 for flow limited paths only, until such time that a modification to the reliability standard can be developed to mitigate the identified technical concern. Transmission Operators and Transmission Service Providers must comply with all other requirements of MOD-029-1a.

⁵² See <http://www.nerc.com/docs/compliance/MOD-029%20letter-AJR%202011MAR03.pdf>

Future of the CMEP

With the completion of the fourth year of mandatory compliance with NERC Reliability Standards, the CMEP has seen a large number of changes take place, and many more are in development for implementation in the coming years. One of the primary goals for 2011 is to transition the audit process away from documentation based standards towards risk and performance-based criteria. The details concerning these efforts are described next.

Risk and Performance-Based Auditing

Beginning in 2011, it was the goal of NERC Compliance Operations to incorporate risk-based and performance-based components into future iterations of the implementation plan for the CMEP. Risk-based and performance-based audit criteria include six components for which the audit scope of a registered entity will be identified. The AML within the implementation plan of the CMEP will represent the minimum audit scope for any given registered entity, but based upon these risk and performance-based components, an audit scope can be expanded to include other reliability standards that are determined to be necessary by an RE after considering a registered entity in light of these components. The risk-based components, or criteria as they may also be called, are as follows:

- North American-wide NERC Reliability Standards most violated, including both all time historical and rolling twelve-month statistics, are considered. This encompasses the core standards to be monitored across the industry.
- RE specific most violated NERC Reliability Standards, which may include standards already identified above for some Regional Entities, or additional standards. This analysis allows REs to focus on significant trends and issues within the RE boundary. This also could lead to the identification of Interconnection-wide issues and concerns.
- RE reliability standards most violated, as applicable.
- Registered entity specific issues, including but not limited to operational issues, operational footprint changes, corporate restructuring, other trends, *etc.*
- Random determination (other high risk reliability standards, registered functions trends and concerns, standards rising in prominence and identified through trend analysis).
- Compliance culture, which considers the entity's compliance culture and overall strength of compliance.

The performance-based approach has two components. One component is the past performance of a registered entity as it relates to the operation of the BPS and the relative strength of the compliance controls in place to assure compliance. The second component includes a more detailed review and testing of the registered entity's programs and procedures to assure actual performance of the stated programs is being implemented, rather than relying solely on documentation.

REs will determine the registered entity's specific audit scope based upon the NERC AML and the six components listed above. The audit scope for registered entities that are registered for

performing identical “functions” will not always be identical across or within the REs. Registered entities will be advised of the audit scope when they receive the formal audit notice. Compliance information and data archived by the RE from the implementation of previous monitoring methods will be utilized in the development of a registered entity’s audit scope, including but not limited to previous audits, self certifications, events, and previous or current enforcement actions.

Implementation of Upcoming Standards

NERC Reliability Standards are in a constant state of change, from the release of new standards entirely to the issuance of new versions of existing standards, some of these changes have the potential for much greater impact to the CMEP than others. Of those that are particularly noteworthy for 2012 and beyond are:

PER-003-1 Operating Personnel Credentials

This standard is an incremental improvement to PER-003-0 with United States enforcement beginning 10/1/2012. It expands on Version 0 of the standard by requiring specific areas of competency and certification for System Operators that are performing real-time operations related to Reliability Coordinator tasks, Transmission Operator Tasks, and Balancing Authority tasks. The standard is now much more explicit regarding the evidence required to demonstrate compliance with the standard. Entities will be expected to provide:

- A list of Real-time operating positions.
- A list of System Operators assigned to its Real-time operating positions.
- Work schedules, work logs, or other equivalent evidence showing which System Operators were assigned to work in Real-time operating positions.
- A copy of each of its System Operator’s NERC certificate or NERC certificate number with expiration date which demonstrates compliance with the applicable Areas of Competency.

FAC-008-3 Facility Ratings

This standard is an incremental improvement to FAC-008-1 with United States enforcement beginning 1/1/2013 (FAC-008-2 was never mandatory and enforceable in any jurisdiction). It retains much of the existing standard, but builds on some of the requirements and adds new requirements. Unlike FAC-008-1, which essentially holds the Generator Owner (GO) and the Transmission Owner (TO) to the same standard, FAC-008-3 has explicit requirements that require the applicable entities have detailed methodologies meeting certain criteria for the ratings of generators, the ratings of the generator lead lines, and the ratings of transmission facilities. These requirements are applicable to the GO, and the TO, respectively. Additionally, the standard now requires that entities implement those methodologies, and that they provide the resultant ratings to various other entities.

FAC-013-2 Assessment of Transfer Capability for the Near-Term Transmission Planning Horizon

This standard is a merging of, and an incremental improvement to, FAC-012-1 and FAC-013-1 with United States enforcement beginning April 1, 2013. In November of 2009, the FERC issued

Order No. 729, in which it directed the ERO to establish a standard that requires the calculation of transfer capabilities in the planning horizon, and ensure that the process used to calculate transfer capabilities in the planning horizon is consistent with the process used in the operating horizon. FERC set a deadline of January 28, 2011 for compliance with their order. In addition to retaining the key elements of FAC-012-1 and FAC-013-1, the new standard includes additional details regarding what is required to be considered within an entity's transfer Capability methodology, and provides an avenue through which entities may request supporting information related to the calculation of transfer capability.

Actively Monitored List

Two noteworthy changes to the 2013 Implementation Plan include:

- Both audit scope and audit periodicity for a registered entity starts with the tier one and the usual audit schedule, but can be adjusted by the RE, with NERC oversight, based upon entity assessment.
- Self certifications of requirements are not necessary during an audit year where those requirements are being audited.

The emphasis in 2013 is moving the entire ERO toward performing quality registered entity assessments. A quality entity assessment includes a risk assessment, a careful look at internal controls, and details of an entity's internal compliance program (ICP). Internal controls are not only based on documentation, but also contain a performance aspect so that an entity is actively monitoring its own compliance. Emphasizing quality registered entity assessments are the key to performance based auditing. When there is confidence in entity assessments, both audit scopes and audit periodicity can be specifically tailored for each registered entity. In 2012 it was emphasized that Tier 1 standards represent minimum audit scope. However in 2013, if an entity's assessment indicates such, either an audit scope can be smaller than Tier 1 or audit periodicity can be reduced. This can allow for more compliance monitoring of entities which pose more risk to the reliability of the BES, which is the heart of performance monitoring.

NERC staff will continue to monitor recent events, such as the southwest cold snap event and the southwest blackout, and the progress of the FFT process as part of the CEI. To date, no changes have been necessary based on these factors. The substantive change in terms of compliance monitoring is that self certifications are not necessary from those entities undergoing an audit in a particular year for the standards requirements that are encompassed by the audit's scope.

Appendix A – Actively Monitored Reliability Standards

The 2011 AML included a total of 39 reliability standards, encompassing 578 associated requirements, to be monitored for purposes of minimum compliance audit scope. In addition to audits, the AML defined the ERO's expectations for self-certifications to which registered entities certify compliance during the compliance year; self-certifications were set for 53 reliability standards and an associated 764 requirements. The ERO designated one reliability standard, encompassing two requirements, as subject to spot check. The following list details which of the reliability standards effective throughout 2011 were applicable to each of these different compliance discovery methods.

2011 CMEP Reliability Standards Summary			
Reliability Standards (FERC Approved)	Self-Certification Annual (A)	Annual Program Audit (X)	Spot Check (SC)
BAL-001-0.1a			
BAL-002-0			
BAL-003-0.1b			
BAL-004-0			
BAL-005-0.1b			
BAL-006-1.1			
CIP-001-1	A	X	
CIP-002-3, Effective 10/1/2010	A	X	
CIP-003-3, Effective 10/1/2010	A	X	
CIP-004-3, Effective 10/1/2010	A	X	
CIP-005-3, Effective 10/1/2010	A	X	
CIP-006-3c, Effective 10/1/2010	A	X	
CIP-007-3, Effective 10/1/2010	A	X	
CIP-008-3, Effective 10/1/2010	A	X	
CIP-009-3, Effective 10/1/2010	A	X	
COM-001-1.1	A	X	
COM-002-2	A	X	
EOP-001-0			
EOP-002-2.1	A	X	
EOP-003-1	A	X	
EOP-004-1			
EOP-005-1	A	X	
EOP-006-1	A		
EOP-008-0	A	X	
EOP-009-0			
FAC-001-0	A		

2011 CMEP Reliability Standards Summary			
Reliability Standards (FERC Approved)	Self-Certification Annual (A)	Annual Program Audit (X)	Spot Check (SC)
FAC-002-0			
FAC-003-1	A	X	
FAC-008-1	A	X	
FAC-009-1	A	X	
FAC-010-2.1 Effective 4/19/2010			
FAC-011-2 Effective 4/29/2009			
FAC-013-1			
FAC-014-2	A		
INT-001-3			
INT-003-2			
INT-004-2			
INT-005-3 Effective 7/1/2010			
INT-006-3 Effective 7/1/2010			
INT-007-1			
INT-008-3 Effective 7/1/2010			
INT-009-1			
INT-010-1			
IRO-001-1.1			
IRO-002-1	A		
IRO-003-2	A		
IRO-004-1	A	X	
IRO-005-2	A	X	
IRO-006-4.1			
IRO-014-1			
IRO-015-1			
IRO-016-1			
MOD-001-1 Effective 4/1/2011	A	X	
MOD-004-1 Effective 4/1/2011	A	X	
MOD-006-0.1 Retired 3/31/2011			
MOD-007-0 Retired 3/31/2011			
MOD-008-1 Effective 4/1/2011	A	X	
MOD-010-0			
MOD-012-0			
MOD-016-1.1			
MOD-017-0.1			
MOD-018-0			
MOD-019-0.1			
MOD-020-0			
MOD-021-0.1			
MOD-028-1 Effective 4/1/2011	A		
MOD-029-1 Effective 4/1/2011	A		
MOD-030-2 Effective 4/1/2011	A		
NUC-001-2 Effective 4/1/2010	A		SC

2011 CMEP Reliability Standards Summary			
Reliability Standards (FERC Approved)	Self-Certification Annual (A)	Annual Program Audit (X)	Spot Check (SC)
PER-001-0.1	A		
PER-002-0	A	X	
PER-003-0	A		
PER-004-1	A	X	
PRC-001-1	A	X	
PRC-004-1	A	X	
PRC-005-1	A	X	
PRC-007-0			
PRC-008-0	A	X	
PRC-009-0			
PRC-010-0			
PRC-011-0	A	X	
PRC-015-0			
PRC-016-0.1			
PRC-017-0	A	X	
PRC-018-1			
PRC-021-1			
PRC-022-1			
PRC-023-1 Effective 7/1/2010	A	X	
TOP-001-1	A		
TOP-002-2a	A	X	
TOP-003-0			
TOP-004-2	A	X	
TOP-005-1.1			
TOP-006-1	A		
TOP-007-0			
TOP-008-1			
TPL-001-0.1	A		
TPL-002-0a	A	X	
TPL-003-0a Effective 4/23/2010	A	X	
TPL-004-0			
VAR-001-1	A	X	
VAR-002-1.1b	A	X	

Appendix B – Compliance Audit Observation Report of Regional Entities

Introduction and Audit Oversight Objectives

NERC compliance auditors maintain oversight of RE compliance audit teams throughout the entire audit process, pre-audit, on-site and post audit. NERC compliance auditors seek to capture compliance applications, positive observations, lessons learned, and recommendations. The primary purpose of the AAO Audit Oversight program is to focus on the compliance monitoring process; however, it is not to make determinations of compliance. NERC's audit oversights are designed to perform a thorough evaluation of the processes and criteria used by all REs in their determination of registered entities' compliance with the NERC Reliability Standards. During compliance audits, NERC staff may identify compliance applications⁵³, positive observations or good auditing practices, lessons learned, and recommendations. NERC communicates the results of its observations for feedback to REs, the development and revision of CANs, RSAWs, Compliance Process Bulletins, ERO auditor training, and compliance workshops for industry.

As NERC compliance auditors observe and participate in future compliance audits, NERC will provide continued compliance guidance to REs and registered entities through various methods. NERC summarizes such methods and compliance applications, positive observations, lessons learned, and recommendations in its 2011 Compliance Audit Observation Report of the REs.

Selection Criteria

In 2011, NERC observed six RE led compliance audits. NERC AAO staff selected compliance audits of registered entities to observe. The 2011 audit observation scheduled included at least two audits within each RE in order to provide oversight to all REs in their conduct of compliance monitoring activities as well as to assist in the evaluation of the REs' consistent implementation of the CMEP.

Within each RE, AAO staff will prioritize the registered entities according to the following technical criteria:

- Organization & Structure – registered for a large number of functions, such as vertically integrated utilities
- Real Time Operations – registered for certified functions, especially Reliability Coordinators

⁵³ Compliance applications are identified through issues noted by NERC compliance auditors during an audit such that NERC should consider providing additional guidance to the Regional Entities and registered entities.

- System Size – includes such aspects as number of interconnections, circuit miles of transmission lines, transmission voltages, peak demand, etc.
- Generation Portfolio – includes number of generating units and type of fuel

In addition to technical criteria, AAO staff considered compliance history and issues surrounding a registered entity. Compliance history and issues refer to past and ongoing violations, investigations, BPS system events and associated spot checks.

2011 AAO Oversight Results

For 2011, NERC attended six RE led compliance audits of registered entities. From these, NERC identified eleven potential compliance applications. A compliance application is an issue that relates to a particular application of a reliability standard that may require additional scrutiny within the ERO in addition to guidance in the form of a CAN or otherwise to ensure consistent application. Of the potential compliance applications, noted, four concerned COM-002, two each were applicable to EOP-008 and EOP-005. Resolution of potential compliance applications followed communication with the NERC Reliability Standards department for future reliability standard revisions and consideration for CAN development.

Positive Observations

Positive observations are aspects of the Regional Entities' audit approach that are noted by NERC observers during an audit to represent behaviors or actions that assist in the implementation of the CMEP. NERC considers and compares noteworthy practices applicable to all REs when determining a positive observation. Those noteworthy positive observations from 2011 follow.

Status Update (Debrief) Tool

The compliance audit team uses a tool used for tracking of requirements covered with determinations of compliance and pending data requests. The tool is shared with the registered entity at the end of each day for officially submitting data requests and for providing the registered entity with a summary of audit progress based on the Reliability Standards reviewed.

Daily Caucus and RSAW review with the Audit Team

The RE compliance audit sub-teams met together at least once a day. Each sub-team presents its RSAWs and the basis for its findings to the entire audit team. Collectively, the audit team makes the final determination of no finding or non-compliance. The daily caucus provides all audit team members the opportunity to fully understand any compliance issues.

Enforcement Turnover

The RE audit team provides a detailed turnover to its enforcement group for any PVs identified during the audit. This turnover provides a narrative that describes the PV and includes references to evidence and data requests used to determine the PV.

Just in Time Training

The RE requires all audit team members to complete the “Just-In-Time” training if audit team members have not completed the training in the last 90 days. The purpose of this training is to refresh fundamental concepts of auditing which supplements training required by NERC.

Recommendations to the Audited Registered Entity

Upon completion of the audit and prior to the exit briefing, the RE compliance audit team holds a session with audited entity’s compliance department personnel to discuss methods and recommendations for improving the registered entity’s compliance program. This is done in conjunction of evaluating the registered entity’s internal compliance program.

Cross-training CIP auditors

The operations and planning compliance audit team included two CIP auditors who were provided the opportunity to learn the audit process and approach with non-CIP reliability standards and is an excellent method for enhancing the knowledge-base and experience of compliance auditors.

FAC-008 and FAC-009 Facility Rating Methodology Checklist

The compliance audit team developed a spreadsheet-based checklist for FAC-008 and FAC-009 Facility Rating Methodology. The checklist ensures that all appropriate equipment is accounted for within an entity’s facility rating methodology as required by FAC-008-1. Additionally, this checklist catalogs the locations within a registered entity’s facility rating methodology relating to ratings for each type of equipment for easy reference when examining data as part of FAC-009-1.

Index Tool for Evidence Identification

To facilitate the logistical considerations of submitted evidence, the RE compliance audit team uses an evidence index tool based upon a spreadsheet and includes this within their audit reports. The RE compliance audit team supplied the audited registered entity with this evidence index such that evidence submitted during the audit process would be cataloged by the registered entity. As a result, AAO staff noted that efficiency of the audit process was gained by both the RE compliance audit team, which did not need to expend its own resources on the cataloging of evidence, as well as for the registered entity, which used the evidence index numbers itself when referring to documentation.

Interview Tracking Tools

The RE employees a tool to track questions developed during its pre-audit review to ask SMEs during the on-site audit. This tool functions as an effective interview audit plan to ensure that interviews are conducted in a methodical and efficient manner.

Lessons Learned

Lessons learned are lessons identified by NERC compliance auditors during the practical execution of audit activities that are helpful for other audit teams to be mindful of during future audits to avoid potential problems and complications. The lessons learned item dealt with the audited entities lack of cohesive evidence. The lessons learned from 2011 audit oversight follow.

Disjointed Documentation:

During the review of documentation for heavy standards, such as FAC-003 and FAC-008, it was found that the registered entity's associated plan and methodologies consisted of several documents rather than having one be all inclusive for each applicable standard or requirement. The documentation was further complicated by a lack of revision histories or references tying them together. Additionally, within its documentation, the entity referred to its regional criteria in many instances but in a haphazard manner, bringing about the situation where only some portions of a program, such as the entity's facility rating methodology, were consistent with these criteria. During the course of the audit, the audit team informed the entity that it should attempt to be consistent with its use and application of regional criteria. The audit team also made a suggestion on how to improve documentation during the audit closing presentation.

Suggestions and Items for Consideration

During the audit process, NERC compliance auditors may notice difficulties encountered by RE audit teams or the registered entity being audited that impede the audit's efficiency or hamper an audit team's ability to determine compliance for a given requirement or reliability standard. As such, NERC recommendations provide compliance auditors guidance to prevent or mitigate re-occurrence of these difficulties in the future. Some of the notable recommendations follow.

Same Corporate Umbrella - Auditing Multiple Registered Entities (different NCR numbers and entity names)

The audited entities referred to themselves in verbal accounts and in documentation with a number of different names which lead to some confusion among the audit team regarding evidence or RSAWs relating to one entity or another.

When this situation is unable to be avoided, AAO staff recommends the audit team should request one set of RSAWs from each entity even if there is to be only one audit report.

Including Guidance within the Audit Notification Packet

The audited registered entity provided narratives in the RSAWs oftentimes did not make connections between requirements and documents used as evidence. More common was the complete absence of references altogether.

The RE compliance audit team mentioned that as part of a recent RE compliance workshop, the RE had provided guidance to those entities in attendance on best practices when completing RSAWs. The audited entity was not present at this workshop.

AAO staff recommends that the RE consider providing this information in either a condensed or complete format within the audit notification packet.

Use of a daily debrief or status update tool

At the close of each day, the RE compliance audit team lead provided a daily debrief to the registered entity that included a verbal overview of the review status for the reliability standards that had been reviewed for the day.

AAO staff notes that a daily debrief is important for the registered entity and for the audit team. In addition to a review status for each standard within the audit scope, the debrief should include identified recommendations and submitted data requests, preferably in written form. This is especially important for audits utilizing multiple audit teams and scribes as other team members are completely reliant on the scribe and openness of the other audit sub-teams to share recommendations and data requests among the entire team. A written daily wrap-up of topics such as those mentioned would help ensure that no confusion or misunderstandings have occurred and that the full audit team is in agreement.

In order to enhance transparency of an audit for the audited entity and all audit team members, AAO staff recommends that RE enhance its daily debriefs with a summary document that lists all standards within the audit scope that clearly specifies the current status of each of those standards in terms of review. At a minimum, the status should describe whether a standard is under review, closed with no finding, or closed with a finding. Additionally, it is recommended that this summary document include the listing of data requests awaiting registered entity responses and tracks recommendations.

Interviewing Techniques

During a Subject Matter Expert (SME) interview, the RE compliance audit team member served as both the lead interviewer and the scribe. This led to some confusion and anxiety on the part of the SME when he finished responding to questions and was left waiting as the interviewer wrote notes without acknowledgement of the SME.

AAO staff recommends that the RE designate one audit team member as a lead interviewer and one as a dedicated scribe for each and every interview session to reduce burden on the registered entity in terms of SME time requirements.

Responsible Person for Presenting Evidence

During the SME evidence review for PRC-008-0 and PRC-023-1, the RE compliance audit team controlled the presentation of evidence, resulting in the SMEs directing the audit team to various documents and places within the documents while standing next to a projection screen. This format resulted in time delays and overall inefficient sessions as the SMEs were left waiting for audit team members to find and open documents as well as to find information within documents under SME direction.

AAO staff recommends that as a general practice, and especially for document and record intense reviews such as FAC-009, PRC-005, PRC-008, PRC-023, *etc.*, the RE compliance audit team have registered entity SMEs control the presentation of evidence in consideration of the fact that SMEs have greater familiarity with the evidence. The burden of demonstrating compliance lies with the registered entity, and this should extend to the provision of evidence as well as its presentation and explanation.

Critical Infrastructure Department (CID)

The implementation by registered entities of compliance measures pertaining to CIP Standards 002—009 continued to mature in 2011, as did the assessment process performed by the ERO. There were no updates to the standards during the year, but the impact of changing standards

did contribute to the decision early in the year for CEAs to consider the standard audit period to be from October 1, 2010; *i.e.*, the effective date of version 3 of CIP Standards 002-009. This approach not only helped registered entities who did not have to focus on preparing and submitting audit evidence for multiple versions of the standards, but also enabled the CEAs to better manage most audits by approaching the review from a single reference point.

Another issue that impacted the assessment of compliance to the CIP Standards 002-009 during 2011 was the CANs that pertained to CIP Standards' requirements. Technologically complex requirements, often impacted by Technical Feasibility Exceptions (TFEs), made it necessary to complete various activities to support TFE assessments and audits according to guidance contained in applicable CANs. However, the long-term result of consistent evaluations remains the focus of the effort.

The ERO CIP auditors from all the Regional Entities continued their joint efforts to identify and resolve issues of common concern, with a goal of approaching issues consistently. The CIP Compliance Working Group (CCWG) used email conversations on the NERC list server with 40-50 messages a month, monthly conference calls, quarterly face to face meetings, and a sub-group dedicated to addressing TFE issues.

A unique opportunity for the CIP auditors presented itself in 2011 when they met with the 706 SDT as it continued work on version 5 of the CIP Standards. The meeting provided both groups a perspective on the work performed by their counterparts, and helped the 706 SDT identify ways to develop standards that are both practical and auditable.

Technical Feasibility Exceptions (TFEs)

In Order No. 706, FERC directed that the ERO submit an annual report with a wide-area analysis regarding use of the TFEs and their impact on BPS reliability. The first "annual" report actually covered the first 18 months of the TFE program, and was submitted on September 30, 2011. Besides narrative content about the program, there were also numerous spreadsheets and tables with data regarding the quantities and types of TFEs that had been submitted, with related data pertaining to those requests.

Various aspects of the TFE program have been considered especially difficult to administer by registered entities and REs alike, in part because the program was developed before its full impact could be determined. As a result, the TFE Managers have identified areas of the TFE Procedure (Appendix 4D to NERC's Rules of Procedure) for which the group would like to propose changes.

Sufficiency

CID's "Sufficiency Review Program" (SRP) grew in popularity and effectiveness in 2011. The SRP provides a "discussion-based dialogue" approach to examine an entity's Risk-Based Assessment Methodology (RBAM) and determine whether it is sufficient to ensure the secure, reliable operation of the BPS. The program reached ten BPS entities in 2011, and added value to the process by giving participants an update to support significant changes to the CIP Standards, in particular, CIP-002-4, Aurora, and including information pertaining to infrastructure protection from the Department of Homeland Security.

2011 Sufficiency Reviews	
Entity	Date
Dayton Power and Light (RFC)	June 20-24, 2011
City of Independence Missouri (SPP)	July 11-12, 2011
Pacific Gas and Electric (WECC)	July 25-29, 2011
Orlando Utilities Commission (FRCC)	August 29th – September 2, 2011
Louisiana Generating (SERC)	December 12-13, 2011
Cottonwood Energy (SERC)	December 12-13, 2011
Cabrillo Power I (WECC)	December 12-13, 2011
Connecticut Jet Power (NPCC)	December 12-13, 2011
Entergy Corporation (SERC)	December 14-16, 2011
Black Hills Electric Cooperative (WECC) - <i>offsite</i>	December 19-21, 2011

Auditor Training Activities

The NERC compliance auditors whose focus is CIP Standards 002 through 009 participated in various training activities during 2011. The Compliance Operations department led two training activities for both the ERO operations and planning compliance auditors, and the ERO CIP compliance auditors. The NERC CID group also led training that focused specifically on consistency and the CIP Standards audit process.

Appendix C – Regulatory Actions

A list of NERC filings to FERC made in 2011 and FERC orders issued in 2011 can be found on the NERC website at <http://www.nerc.com/page.php?cid=1|9|170>.

CIP-005 Compliance Analysis Report

Action

Accept the CIP-005 Compliance Analysis Report.

Background

CIP-005 is a NERC Reliability Standard that is critical to the reliability of the bulk power system (BPS). NERC worked with the Regional Entities (REs), the Compliance and Certification Committee (CCC), and the Critical Infrastructure Committee (CIPC) to provide meaningful comments to the development of this report. To date, this is the most comprehensive Compliance Analysis Report and offers great suggestions for compliance for registered entities, as well as the usual violation statistics and violation description examples.

Summary

This summary is intended to capture the analysis detailed below by providing some essential elements of the requirements, and by offering some suggestions for consideration. It is not a complete list of all possible elements or actions. Evaluation or undertaking such actions or suggestions does not guarantee compliance and does not replace the NERC Reliability Standards language. "Suggested Enhancements" are included for informational purposes only.

The expectation with the CIP-005 standard is that Critical Asset identification drives the process, not the Critical Cyber Asset identification. The CIP-005 standard also suggests that the Critical Asset and Critical Cyber Asset identification process feeds into the Electronic Security Perimeter (ESP) identification, implementation, monitoring and vulnerability processes. The registered entity thus may wish to consider the following order of steps for establishing compliance to CIP-005:

1. Identifying critical assets
2. Identifying critical cyber assets
3. Designing the ESP
4. Identifying everything else within the ESP
5. Identifying the ESP access points
6. Identifying the cyber assets that perform access control and monitoring of the ESP
7. Performing annually a cyber vulnerability assessment of all the electronic access points to the ESP
8. Documenting the results of the identification and implementation process

There are currently 369 possible violations all-time, with 249 of them occurring in the last 12 months. The 249 possible violations rank second only behind CIP-007. It is encouraging to see that 66 percent of CIP-005 violations were self-identified.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-005 Compliance Analysis Report

Electronic Security Perimeter(s)

May 2012

RELIABILITY | ACCOUNTABILITY



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

Table of Contents

Table of Contents	1
NERC's Mission	i
ERO Compliance Analysis Reports.....	1
Summary of Practical Information and Suggestions	2
CIP-005 Background Information	3
CIP-005 Compliance	4
Critical Asset Identification	4
Critical Cyber Asset Identification	4
Designing the ESP	5
Identifying the ESP Access Points.....	5
Monitoring and Logging Electronic Access	6
Vulnerability Assessment	6
CIP-005 Violations by Method of Discovery.....	7
CIP-005 Violations by Region	8
CIP-005 Violations by Requirement	9
Detailed Requirement R1 Violation Information	10
Detailed Requirement R2 Violation Information	14
Detailed Requirement R3 Violation Information	18
Detailed Requirement R4 Violation Information	21
Detailed Requirement R5 Violation Information	25
Conclusion	27

NERC's Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to enhance the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; assesses adequacy annually via a 10 year forecast and winter and summer forecasts; monitors the BPS; and educates, trains, and certifies industry personnel. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.¹

NERC assesses and reports on the reliability and adequacy of the North American BPS, which is divided into eight regional areas, as shown on the map and table below. The users, owners, and operators of the BPS within these areas account for virtually all the electricity supplied in the U.S., Canada, and a portion of Baja California Norte, México.

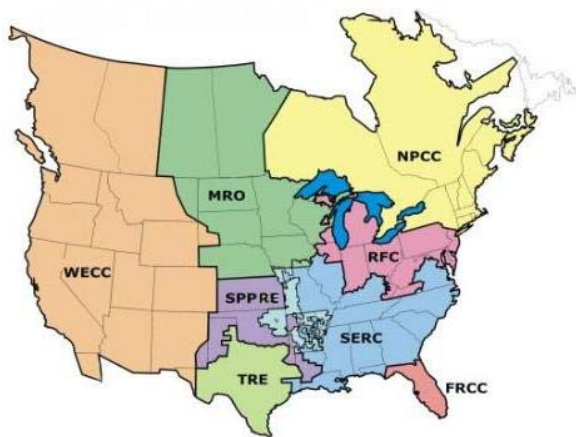


Table A: NERC Regional Entities

FRCC Florida Reliability Coordinating Council	SERC SERC Reliability Corporation
MRO Midwest Reliability Organization	SPP Southwest Power Pool, Incorporated
NPCC Northeast Power Coordinating Council	TRE Texas Reliability Entity
RFC ReliabilityFirst Corporation	WECC Western Electricity Coordinating Council

Note: The highlighted area between SPP and SERC denotes overlapping regional area boundaries: For example, some load serving entities participate in one region and their associated transmission owner/operators in another.

¹ As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the "electric reliability organization" under Alberta's Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the Régie de l'énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. NERC's reliability standards are also mandatory in Nova Scotia and British Columbia. NERC is working with the other governmental authorities in Canada to achieve equivalent recognition.

ERO Compliance Analysis Reports

As the Federal Energy Regulatory Commission (FERC) certified² Electric Reliability Organization (ERO) and pursuant to Section 215 of the Federal Power Act and the FERC approved Rules of Procedure (ROP)³; the Compliance Monitoring and Enforcement Program (CMEP) and Organizational Registration and Certification Program, NERC is responsible for the registration and certification of users, owners and operators of the BPS.

To provide guidance and information to the industry, NERC announces and posts [Compliance Analysis Reports](#). To date, NERC has posted 11 of these reports that focus on highly violated standards and those important to the reliability of the BPS. NERC has also posted two reports that focus on the ERO and Regional Entity Organization Registration and Certification Programs. The 11 reports that have been issued are:

- PRC-005
- CIP-004
- FAC-008 & FAC-009
- CIP-001
- VAR-002
- PER-002
- CIP-006 & CIP-007
- EOP-005
- TOP-002
- ERO Registrations and Registration Appeals
- ERO Certifications

² Energy Policy Act of 2005 - Section 215 FERC Implementing Rule – 18CFR39 (Order 672)

³ NERC Rules of Procedure Effective: March 15, 2012

Summary of Practical Information and Suggestions

This summary is intended to capture the analysis detailed below by providing some essential elements of the requirements, and by offering some suggestions for consideration. It is not a complete list of all possible elements or actions.

Evaluation or undertaking such actions or suggestions does not guarantee compliance and does not replace the NERC Reliability Standards language. “Suggested Enhancements” are included for informational purposes only.

The purpose of CIP-005 is to identify and protect the Electronic Security Perimeter inside which all Critical Cyber Assets reside as well as all access points on the perimeter

The process steps for CIP-005 are:

1. Identifying the Critical Assets
2. Identifying Critical Cyber Assets
3. Designing the Electronic Security Perimeter (ESP)
4. Identifying everything else within the ESP
5. Identifying the ESP access points
6. Identifying the Cyber Assets that perform access control and monitoring of the ESP
7. Performing annually a cyber vulnerability assessment of all the electronic access points to the ESP
8. Documenting the results of the identification and implementation process

A detailed level of review for the steps listed above is included later in this report.

There are currently 369 possible violations all-time, with 249 of them occurring in the last 12 months. The 249 possible violations rank second only behind CIP-007. It is noteworthy that 66% of CIP-005 violations were self-identified.

CIP-005 Background Information

The current version of this reliability standard is CIP-005-3. CIP-005-4 was approved by the NERC Board of Trustees (BOT) in January of 2011. It will become effective the first day of the eighth calendar quarter after applicable regulatory approvals have been received (otherwise the reliability standard becomes effective the first day of the ninth calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).

CIP-005 has five high level Requirements and 26 sub-level Requirements. It is important to note that all violations discussed in this report will be a collective roll-up of all versions of CIP-005, and the date of all violations is through December 31, 2011.

From a violation standpoint, CIP-005's 369 violations rank sixth all-time. In the past 12 months, CIP-005's 249 violations ranked second only behind CIP-007. All CIP standards besides CIP-008 are ranked in the top 10 most violated standards in the past 12 months.

Table 1: Top 10 Violated NERC Reliability Standards through December 31, 2011

Top 10 Violations			
All-Time		Previous 12 Months	
Standard	Violations	Standard	Violations
PRC-005	817	CIP-007	500
CIP-007	787	CIP-005	249
CIP-004	511	CIP-006	242
CIP-001	459	PRC-005	214
CIP-006	387	CIP-004	164
CIP-005	369	CIP-003	117
CIP-003	237	CIP-002	112
VAR-002	236	VAR-002	100
CIP-002	209	CIP-001	61
FAC-008	206	CIP-009	51

CIP-005 Compliance

The expectation with the CIP-005 standard is that Critical Asset identification drives the process, not the Critical Cyber Asset identification. The process steps are:

1. Identifying the Critical Assets
2. Identifying Critical Cyber Assets
3. Designing the ESP
4. Identifying everything else within the ESP
5. Identifying the ESP access points
6. Identifying the Cyber Assets that perform access control and monitoring of the ESP
7. Performing annually a cyber vulnerability assessment of all the electronic access points to the ESP
8. Documenting the results of the identification and implementation process

Critical Asset Identification

Critical Asset identification CIP-002-3, Requirement R2 (R2) is performed through the application of a risk-based assessment methodology per CIP-002-3, R1. Entities shall apply the risk-based assessment methodology at least annually to determine an entity's Critical Asset list. Once this list is developed, entities shall use this list initially to develop and annually update an associated Critical Cyber Asset list.

Critical Cyber Asset Identification

Critical Cyber Asset identification is performed through CIP-002-3, R3. Special attention to:

- Cyber Asset and Critical Cyber Asset definitions that are found in the Glossary of Terms Used in NERC Reliability Standards
- The three qualifying criteria found in CIP-002-3, R3 for identifying Critical Cyber Assets include having at least one of the following characteristics:
 - Use of a routable protocol to communicate outside of the ESP.⁴
 - The communication path between discrete ESPs is excluded. CIP-005 R1.3 notes "communication links connecting discrete ESPs shall not be considered part of the ESP."
 - Use of a routable protocol within a control center
 - Dial-up accessibility

⁴ Note: Identifying Cyber Assets that use a routable protocol to communicate outside of the ESP is problematic at this point because the ESP likely has not been defined yet. The *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets* refers to a "preliminary" ESP in order to get around this issue.

Designing the ESP

The ESP is the logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled. A Critical Asset can also have one or more ESPs that enclose and protect Critical Cyber Assets. ESPs spanning geographically separated Critical Assets are not recommended. A Cyber Asset on the same or subordinate network segments also is included within the ESP design. Anything directly connected to a Cyber Asset within an ESP is also within the ESP (or is designated as an access point).

Identifying the ESP Access Points

If traffic enters or leaves the ESP, there is an associated access point allowing for that communication flow. Access points for consideration include, but are not limited to, the following device types:

- Firewalls
- Routers
- Layer 3 switches
- Layer 2 switches
- Dial-Up Modems
- Wireless access points
- Dual-homed PCs/Servers
- Intrusion Detection/Protection System sensors
- Virtualization (e.g., network communication devices supporting Virtual LANs)

Identifying the Access Control and Monitoring Cyber Assets

Entities shall identify Cyber Assets that perform access control and/or monitoring of the ESP. Additionally an entity shall include these Cyber Assets within the documentation associated with the identified ESP. This identification process can help an entity identify the subset of Cyber Assets that require the afforded protective measures as specified in the CIP-003-3 through CIP-009-3 reliability standards. Access control and/or monitoring solutions for consideration include, but are not limited to, the following device types:

- Two-Factor authentication systems for ESP external interactive access
- Security Information and Event Management (SIEM) and Log Management Solutions
- Virtualization Technologies
- Intrusion Detection and Prevention Systems
- Jump Servers
- Remote Desktops
- Identity Management and Directory Services Solutions

Documenting the Results of the Identification and Implementation Process

For each ESP, it is important to document:

- Each Cyber Asset, both Critical and non-critical within the ESP
- Each ESP access point
- Each electronic access control system
- Each electronic access monitoring/logging system, including those outside the ESP
- Pictorial presentations can help to provide a high-level illustration of the ESP, with details needed for completeness documented within the diagram or separately
 - An example: IP addresses, model numbers, serial numbers, property tag numbers, system names – unique information
- Remember to properly classify the documents for information protection

It is important to stress on asset inventory, even going back to identifying a Critical Cyber Asset. This should include more emphasis on asset discovery including physical walk-downs. For R1.5 with regards to electronic access control and monitoring (EACM) it should include all systems involved in R2.4 (e.g. VPN, citrix, R2.5.2 (RSA, AD, TACACS, RADIUS), and R3 (logging and monitoring systems).

Monitoring and Logging Electronic Access

Entities must monitor and log access at each ESP access point. This includes the dial-up access points to dial-up accessible Critical Cyber Assets. Entities shall develop, document and implement security monitoring processes that detect and alert for attempted or actual unauthorized electronic access. The process shall include the appropriate response personnel, notification steps for the prompt evaluation of the alert, and the appropriate response. The standard requires the ability to monitor “actual unauthorized electronic access”. This infers that entities must log permitted traffic and not just denied traffic.

If the system associated with this process cannot technically detect and alert for an attempted or actual unauthorized electronic access, an entity shall review access logs for an attempted or actual unauthorized access at least every 90 calendar days. Lastly, it would be prudent that entities keep records and documentation associated with all of their ESP monitoring processes for the duration specified in the NERC CIP standard.

Vulnerability Assessment

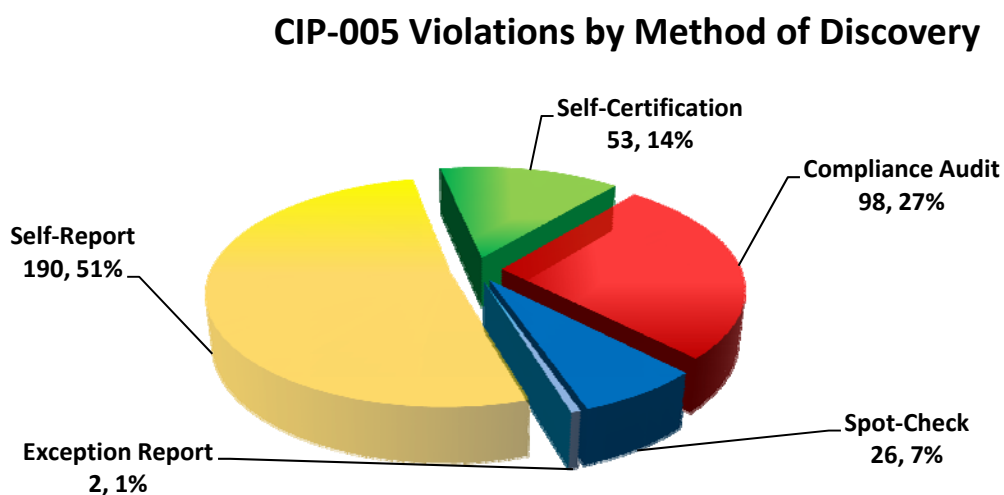
The vulnerability assessment process must be documented. The documentation shall show the verification that only the ports and services required for operations at the access point be enabled. Additionally, the entity shall verify that the controls related to default accounts, passwords, and network management community strings are implemented and working as configured. Lastly, the documentation shall include not only the results of the assessment, but also the action plan to remediate or mitigate vulnerabilities identified and to include an up-to-date execution status of the action plan.

CIP-005 Violations by Method of Discovery

As with any NERC Reliability Standard, self-identifying possible violations are a proactive way a registered entity can promote a reliable BPS. It displays a vigorous internal compliance program (ICP) and shows the entity is doing its self due diligence to routinely review its processes, programs, procedures and execution of those processes, programs and procedures.

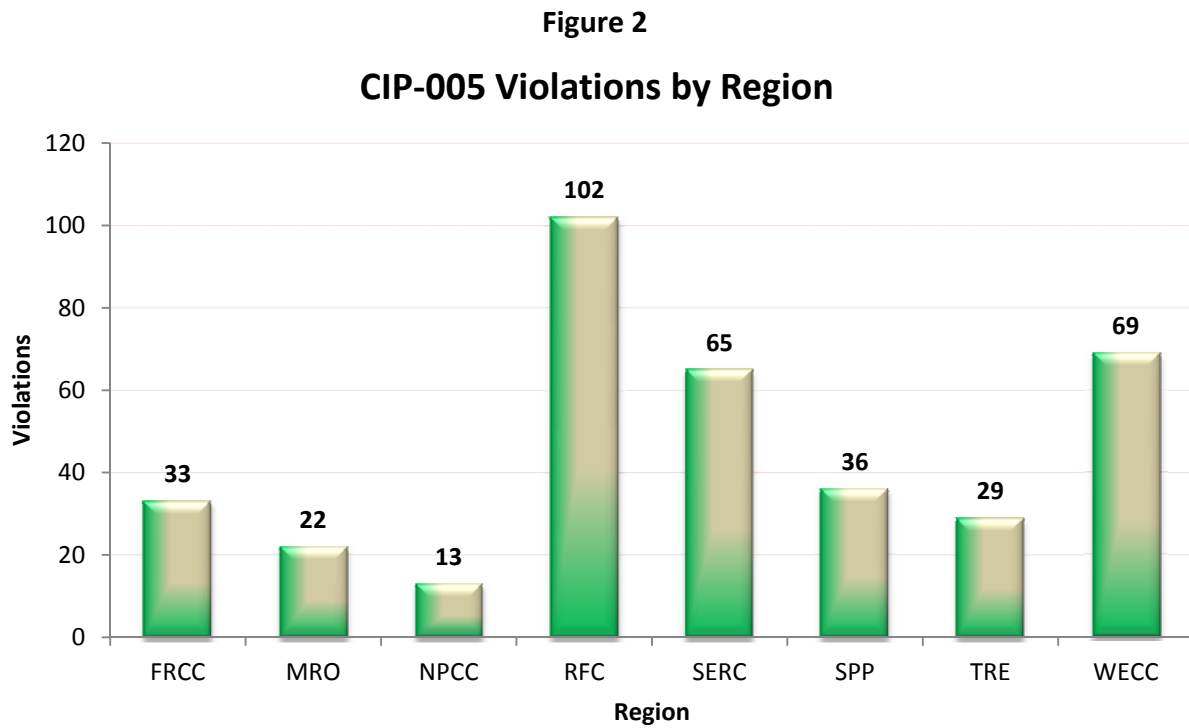
With cyber security a top priority to defend North America against a cyber attack, it is encouraging to see that 66% of CIP-005 violations are self-identified. Self-identified violations come in the form of self-reports, self-certifications, periodic data submittals, and exception reports. The pie chart below in Figure 1 shows the violations by method of discovery.

Figure 1



CIP-005 Violations by Region

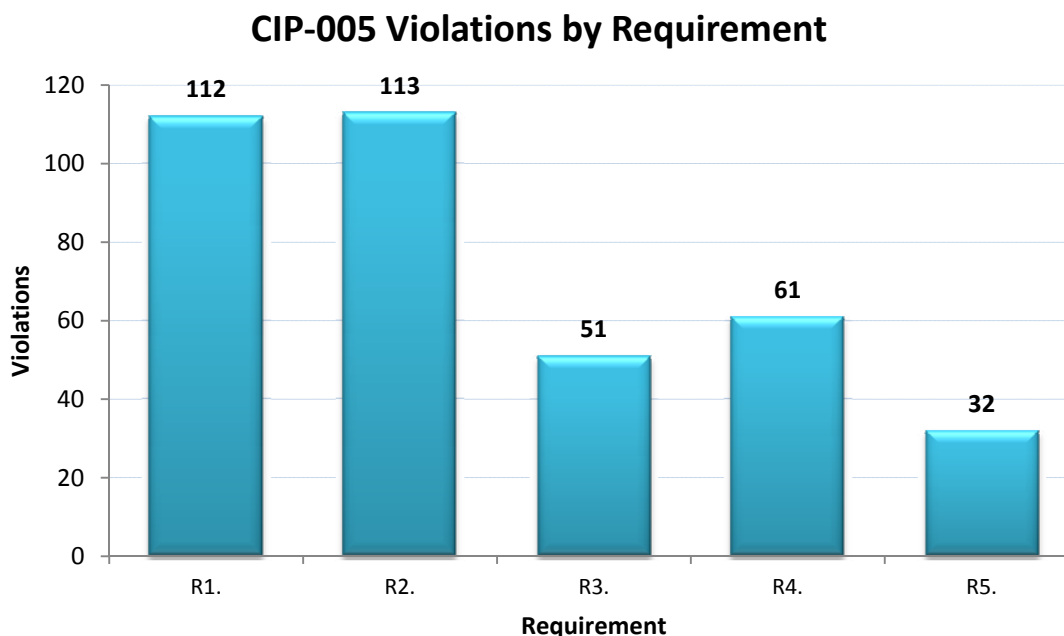
Below is a chart that shows the violations by Region.



CIP-005 Violations by Requirement

CIP-005 has five high level Requirements and 26 sub-level Requirements.

Figure 3

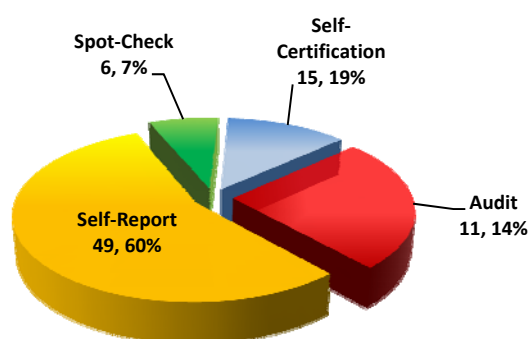


CIP-005 Violations by Requirement	Violations	Percentage
R1 – Electronic Security Perimeter: The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter.	112	30.4%
R2 – Electric Access Controls: The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	113	29.3%
R3 – Monitoring Electronic Access: The Responsible Entity shall implement and document electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	51	16.3%
R4 – Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually.	61	14.9%
R5 – Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	32	9.1%
Total	369	100%

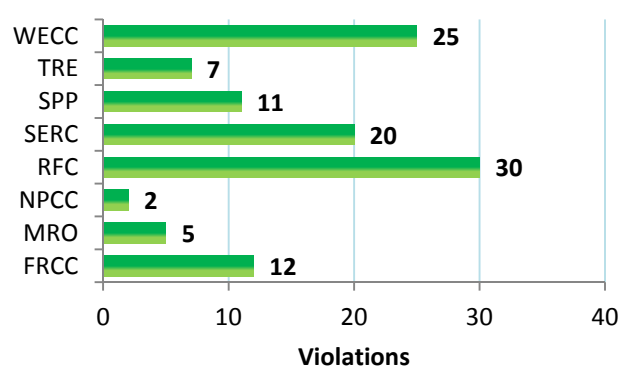
Detailed Requirement R1 Violation Information

CIP-005 Violations by Requirement	Violations	Percentage
R1 – Electronic Security Perimeter: The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter.	112	30.4%
Total	369	100%

R1 Violations by Method of Discovery



R1 Violations by Region



Violation Description Examples

- The entity discovered several devices that had console routers connected to their management ports that were not located within an ESP.
- The entity failed to identify certain non-critical software components installed on certain Cyber Assets within the entity's ESP.
- The entity has switches connected to multiple networks that are communicating outside of the respected ESP, and that are not identified as access points to the ESP.
- Entity self-reported that the use of an improved network scanning tool uncovered a previously undocumented Cyber Asset within an ESP.
- R1 - Entity evidence was insufficient to demonstrate that entity documented all Critical Cyber Assets within the ESP. Entity's ESP Logical drawings did not identify and document all access points to the ESP, specifically the outgoing communication end points for substations that communicate using serial protocol. Further, the entity did not document its ESP and associated access points until June 4, 2010 for requirement with the compliance date of July 1, 2009. R1.5 - Entity evidence was insufficient to demonstrate that all Cyber Assets used in the access control and/or monitoring of the ESP(s) were afforded the protective measures as specified in Standard CIP-003-3, Standard CIP-004-3 R3, Standard CIP-005-3 R2 and R3, Standard CIP-006-3 R3, Standard CIP-007-3, R1 and R3

through R9, Standard CIP-008-3, and Standard CIP-009-3. Specifically, a Web Server was not identified as an access control and monitoring device. This server is used for controlling, monitoring, and triggering alerts. Entity's recovery plan did not include the steps or procedures for recovering all of the access control and monitoring devices. An email documenting the steps was received by the entity during the audit but the entity recovery plan did not include these steps (CIP-009). All EACM devices did not include strong authentication controls for remote access and banners for remote interactive access (CIP-005, R2.4 and R2.6).

Case Notes

There are three Case Notes for R1: CIP-005-2 R1.5, CIP-005-2 R1, and CIP-005-2 R1.4.

Suggested Enhancements

Critical Cyber Assets determine the extent of the ESP

A common error is to presume an ESP and then identify Critical Cyber Assets from the set of Cyber Assets connected to the network segments encompassed by the ESP. Performing the steps out of sequence in this manner could result in Cyber Assets essential to the reliable operation of the Critical Asset not being identified as Critical Cyber Assets because of their placement on the network. Ensure all Cyber Assets (e.g., servers and workstations) essential to the reliable operation of the Critical Asset are identified, and then draw the ESP(s) to encompass all of the identified Critical Cyber Assets. Entities may want to move a Cyber Asset from one network segment to another in order to define a manageable ESP.

Electronic Access Control Points cannot be Critical Cyber Assets

When identifying the Cyber Assets that are essential to the reliable operation of the Critical Asset, certain Cyber Assets on the boundary of the network are candidates to become electronic access points. These are generally communication network devices, such as layer 3 switches, firewalls, or routers. Some layer 2 switches can be configured with rudimentary access control, such as port security (MAC address validation), and can be identified as electronic access points. A common error in the control center is to identify the SCADA Communications Front End systems (CFEs) as electronic access points. Unless the server or workstation is "dual-homed" (directly connected to a routable network within the ESP and also directly connected to an external, non-ESP routable network such as printers, scanners, workstations, servers, etc.) the Cyber Asset is not generally identified as the electronic access point. Entities should carefully review all devices within an ESP to ensure such devices are not also connected to a non-ESP network as mentioned above.

Non-routable data traffic crossing an ESP boundary requires an electronic access point somewhere

A common error is to presume that an electronic access point is only required for routable networks. In fact, any data traffic that crosses the ESP requires an electronic access point somewhere. Some examples include:

1. Field systems communicate with the control center using a serial, point-to-point communications circuit that terminates in a bank of modems or serial-to-Ethernet

converter devices in the control center. The modem or protocol converter devices are likely candidates for the electronic access point.

2. Field systems communicate with the control center over digital, serial communication circuits that terminate directly on a serial expansion port device connected to the CFE server. The CFE is a component in the FEP as well as the digital switch and modems. While the server is a Critical Cyber Asset, the expansion device connected to the CFE is the likely electronic access point.
3. Field systems communicate with the control center over a non-routable communications circuit that includes a signal splitting device. The signal splitting device is commonly used to send the real-time operational data to both the production and the test SCADA systems while allowing only data from the production SCADA system to be sent to the field system. This device is a likely electronic access point.

Sometimes there are multiple options. It is recommended to choose the device that best meets the requirements of the CIP standards. Entities should think creatively on how each candidate device can conform to the CIP standards' requirements. For example, as these devices typically do not support user accounts, they are compliant with the requirements of CIP-007, R5 (Account Management). The requirement, for example, to change passwords annually only applies to user account passwords, of which there are none. Similarly, there are typically no patches for these devices, thus there are none to assess within 30 calendar days of availability. In some cases, a requirement such as CIP-007, R4 (Malicious Software Prevention) cannot be complied with. In those instances, Technical Feasibility Exceptions are applicable and should be requested.

Document the ESP(s), the access points, and the Cyber Assets therein

Documentation can be in the form of network diagrams, tabular lists, or a combination of both. Regardless, document in sufficient detail to ensure all Cyber Assets are accounted for. If documented using network diagrams, ensure the electronic access points are clearly identified and ensure redundancy of Cyber Assets is accounted for. Entities should be sure to examine the ESP diagrams for completeness and accuracy. If a network or communications path crosses the ESP boundary, entities should identify the associated access point. Also, entities should be able to identify all non-critical Cyber Assets within an ESP.

Pay attention to VPN termination points

If the VPN tunnel is passed through the defined electronic access point and terminates on a Cyber Asset within the ESP, that termination point is another electronic access point. A better practice is to terminate the VPN session in a DMZ just outside the ESP and then allow the defined electronic access point to manage the access control of that session's data into the ESP.

Maintain Documentation

As Cyber Assets are added, replaced, or removed, or network changes are made, make sure the CIP-005, R1 ESP documentation is updated. A possible violation may result if the ESP documentation does not match the current configuration. Whenever possible, self-maintain the documentation. Possible violations have been found when the registered entity relied upon a third-party vendor, such as the SCADA system vendor, to maintain the documentation and the documentation was not updated properly or in a timely manner.

Internal Controls

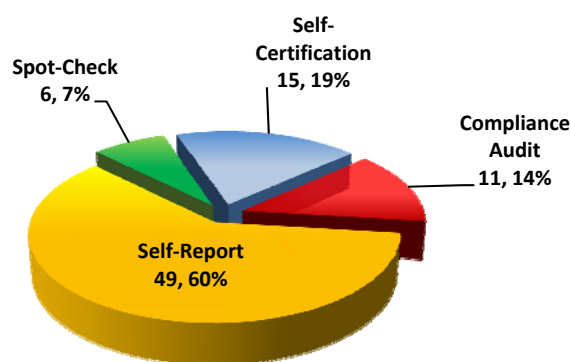
An entity should have a system of internal controls to ensure all Cyber Assets within an ESP are identified, documented and protected.

- In a case where a network is not completely enclosed by a Physical Security Perimeter (PSP), the entity must provide alternative security measures and request a Technical Feasibility Exception (TFE). Examples include cable runs between discrete PSPs and wireless connections between discrete PSPs.

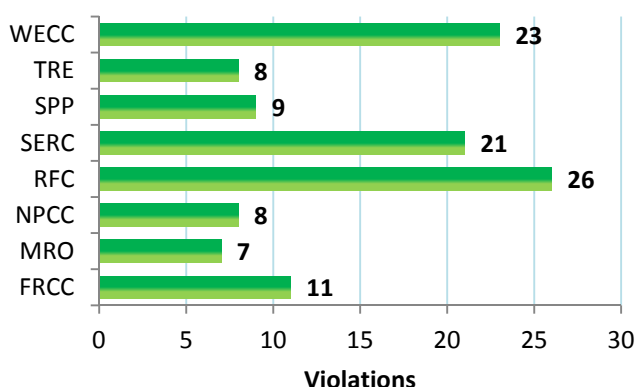
Detailed Requirement R2 Violation Information

CIP-005 Violations by Requirement	Violations	Percentage
R2 – Electric 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).	113	29.3%
Total	369	100%

R2 Violations by Method of Discovery



R2 Violations by Region



Violation Description Examples

- Entity failed to document the configuration of those ports and services required for operations and for monitoring Cyber Assets within their ESP.
- The entity had no documented evidence to show that only ports and services required for operations and monitoring of Critical Assets within the ESP were enabled. In addition, the content of banners was not maintained in a formal, dated document between July 1, 2009 and December 17, 2010.
- Remote desktop protocol (RDP) was available through a perimeter access point that allowed user access from outside the ESP to a Critical Cyber Asset located within the ESP without ensuring authenticity of the user accessing the device. A user had access to a device outside the ESP, and then used RDP to connect to a device within the ESP without uniquely identifying themselves. The issue was discovered during a firewall rule-set review on January 25, 2010.

- There is no documentation supporting the firewall rules for certain firewalls. Documentation is necessary to demonstrate that the defined port or service is required for operations and for monitoring Cyber Assets within the ESP.
- Entity's Account Management Procedure may have been deficient prior to September 20, 2010 regarding the adding/modifying/terminating of user access and language regarding specific timing of said actions.
- The entity failed to provide evidence that explicit access permissions were used as part of their access control model such that only ports and services necessary for operations or monitoring were enabled.

Case Notes

There are two Case Notes for R2: CIP-005-1 R2 and CIP-005-3 R2.4.

Suggested Enhancements

Deny all access by default

CIP-005-3, R2.1 requires the use of a deny-by-default model such that explicit permissions must be specified. These explicit permissions should be as narrowly defined as possible. For example, instead of permitting a Cyber Asset (or all Cyber Assets assigned to the same Class C address space) access to anything within the ESP, each individual Cyber Asset should be explicitly permitted to only the Cyber Assets within the ESP for which access is required. Further narrowing the access permissions, the Cyber Asset access should be limited to specific logical ports. For example, if a Manager's workstation is allowed to access the SCADA system's Human-Machine Interface (HMI) via a secure web interface (Port 443), then code an Access Control List (ACL) statement that explicitly permits the Manager's workstation's IP address access to the HMI Server IP address using port 443 (HTTP/S).

In some firewalls, such as the Cisco devices, security levels are typically assigned to various network segments. Be aware that a higher security level is permitted access to all lower security level networks, overriding the implied default denial. The most protected networks should be assigned the higher security levels.

Finally, some ACLs include an implied Deny-All-All. Entities should still consider coding an explicit Deny-All-All at the end of the ACL, especially where the entity is defining ACL sub-lists associated with an interface, to ensure the default denial is configured as intended.

Document a ports and services baseline

As both CIP-005-3, R2.2 and CIP-007-3, R2.1 require unnecessary ports and services to be disabled, the entity needs to be able to demonstrate that it has been properly done. To be able to demonstrate only the necessary ports and services are enabled, baseline ports and services should be defined. The baseline documentations may group similar devices, such as operator consoles. The baseline documentation should identify each port or service required and the reason it is required. Without a baseline configuration to demonstrate the need has been identified, it is very difficult to demonstrate that only the required ports and services have been

enabled. This baseline is also helpful when performing the CIP-007-3, R1 security controls testing and the CIP-005-3, R4.2 and CIP-007-3, R8.2 vulnerability assessment procedures.

Enable only the ports and services required for operations and for monitoring Cyber Assets within the ESP

Unlike ports and services defined on a Cyber Asset within the ESP (required by CIP-007-3, Requirement R2), there are two types of ports and services that must be addressed with respect to EACM systems. Like the Cyber Asset within the ESP, any unnecessary ports and services that may be offered by the device itself must be disabled. For example, the firewall may permit administrators to connect via Telnet, SSH, or even a web interface (HTTP and/or HTTP/S). If the administrators are expected to connect to the firewall only using SSH and the device can be configured with Telnet and SSH, the Telnet service needs to be disabled (and thus port 23).

The second types of ports of concern are the ports associated with traffic permitted through the electronic access control device. This is normally handled by properly implementing the deny-by-default model. But, to cite another example, if there is a web service running within the ESP that the entity does not want anyone outside of the ESP to access, coding an explicit deny statement that disallows any port 80 (HTTP) or port 443 (HTTP/S) traffic into the ESP should be considered.

Secure dial-up access

Dial-up access occurs when, using modems, a phone number is dialed, is answered by the far-end modem, and a connection is established. This is not an analog or digital point-to-point circuit in which the circuit is normally up and connection established. Dial-up access is often used for out-of-band or remote access to a Cyber Asset, typically for maintenance purposes. There are a number of ways dial-up access can be secured. Examples include:

1. Dial-up authentication system. These devices answer the call and perform user authentication before allowing the caller to connect to the Cyber Asset. In some cases, the authentication system will dial back to the caller at a pre-defined phone number for greater security.
2. Mdem power control. The modem is plugged into a small switch device that can be controlled by the RTU or relay in the remotely accessed site. Typically, the relay technician or other remote user contacts the control center operator who, in turn, issues a close command to the switch device to turn the modem power on. When work is complete, the control center operator issues an open command to the switch to turn it back off. Ideally, some sort of caller identity verification is performed before the modem is enabled.

Authenticate interactive access into the ESP

Strong procedural or technical authentication is required before interactive access is allowed through the electronic access point. Typically, this is performed via a Radius or TACACS+ server interface. The authentication can be initiated by the electronic access control system (e.g., firewall) itself. Another common approach is to have the remote user authenticate to and establish a VPN session that terminates in a DMZ outside of the ESP. As a result of the VPN session authentication, which must be strong itself for this approach to work, the remote user is

assigned a certain IP address. The IP address can be uniquely and permanently assigned to the remote user (best practice) or can be dynamically assigned from a reserved pool of addresses. This assigned address signals the firewall that the user has been strongly authenticated for access. The firewall is configured to allow these assigned IP addresses into the ESP in lieu of performing the authentication itself. When used in this manner, the authentication server and the VPN concentrator collectively is also considered an EACM system and is subject to CIP-005, including R1.5.

Procedural authentication is more difficult and is often used in concert with technical controls. Examples include manually enabling the router interface or dial-up modem after procedurally authenticating the remote user (e.g., vendor support staff) requesting access. Some entities rely upon the Radius or TACACS+ authentication, but the entity physically controls the access token generator while the caller knows the token generator's associated pin code. In that manner, the entity has positive control over allowing the remote user to access the protected Cyber Assets.

Acceptable Use Banner

A common error is to assume the banner must only be displayed upon successful log-in, which is the only capability for some Cyber Assets. Another common error is to rely upon the target end host Cyber Asset to display the acceptable use banner. The standard requires the electronic access control system to display the banner upon all interactive access attempts, including failed attempts. This could include the Radius or TACACS+ server performing the strong technical authentication. Typically, compliant devices display the banner prior to prompting for the user's authentication credentials.

Entities need to document the content of the banner that is to be displayed. This is typically done as part of the cyber security policy or device configuration documentation, and should be separate from a screen capture or configuration file listing from the electronic access control system itself. Where it is not possible to display the banner upon all interactive access attempts, a Technical Feasibility Exception request should be requested to provide safe harbor from a possible violation.

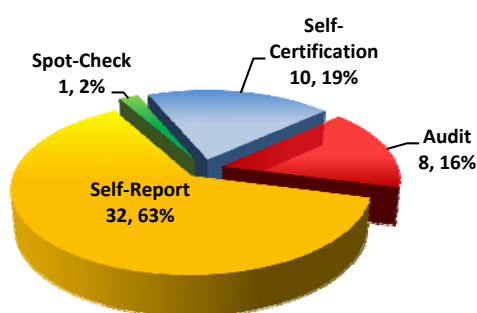
CIP-005-3 R2.2 and CIP-005-3 R4.2

Compliance with these two Requirements should be coordinated as they address similar issues.

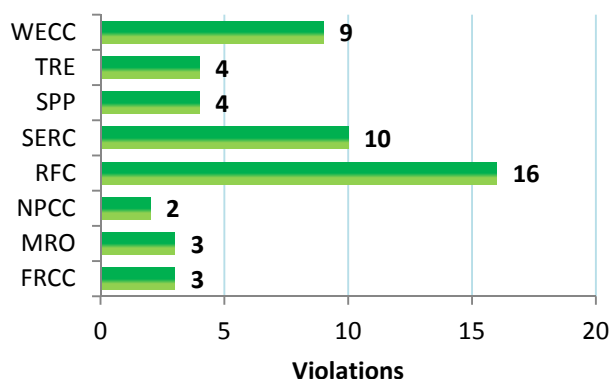
Detailed Requirement R3 Violation Information

CIP-005 Violations by Requirement	Violations	Percentage
R3 – Monitoring Electronic Access: The Responsible Entity shall implement and document electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	51	16.3%
Total	369	100%

R3 Violations by Method of Discovery



R3 Violations by Region



Violation Description Examples

- The entity discovered that “alerting” for unauthorized access attempts had not been enabled on interior firewalls.
- Entity self reported that one technically feasible electronic security access point’s operating system logs were not being monitored or alerted on for attempts at or actual unauthorized access as required by CIP-005 R3.2.
- The entity self reported that the entity failed to implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Critical Cyber Assets (s) twenty-four hours a day, seven days a week as required by CIP 005 R3.
- Entity has some ESP access points without the capability of automated invalid access attempt notification and the access logs were not manually reviewed within 90 days as required.

Case Notes

There are three Case Notes for R3: CIP-005-1 R3, CIP-005-1, R3 and CIP-005-3 R3.2.

Suggested Enhancements

What to Log

The standard requires the ability to monitor “actual unauthorized electronic access.” This infers that entities must log permitted traffic and not just denied traffic. If the entity has not logged successful access then it has not logged “actual” unauthorized access. The bottom line is that entities should log as much as possible. While it could consume significant storage, detailed logs serve as a valuable source of forensic information. During the pre-attack surveillance phase or the actual attack itself, the forensic information may be instrumental in detecting an attack in planning or in progress. Early detection is a prerequisite to being able to deflect an attack and minimize damage. Should an attack be successful, the forensic information will help entities identify the scope of the attack and enable recovery.

Control Center Environment

Manual log reviews are often impractical in a control center environment. Control center firewalls typically generate in excess of 100,000 log entries per day, per firewall. To effectively manage this amount of log data, entities should consider installing and configuring a log aggregation (syslog) and security incident and event management (SIEM) solution. These systems work in concert to collect system event logs from the protected Cyber Assets and analyze them, looking for anomalous network traffic or system activity. Events that exceed pre-defined thresholds (e.g., too many failed log-in attempts over a discrete timeframe), trigger an automated alert to appropriate response personnel.

SIEM solutions need to be configured to minimize false alarms. While they may come preconfigured with a number of alerts, the alert thresholds often need to be configured to the entity’s specific environment. Entities want to eliminate the nuisance alarms, yet do not want to configure the SIEM so loosely that important events are missed. It is not uncommon to take up to a year to get the SIEM solution working smoothly with alerts being issued appropriately.

Entities also typically install Intrusion Detection and/or Intrusion Prevention Systems (IDS/IPS). The Network Intrusion Detection System (NIDS) is designed to look for certain network traffic signatures and to issue alerts. The Network IPS goes one step further and blocks the traffic from going further. Like anti-malware solutions required by CIP-007, R4, the signature files of the NIDS need to be tested before enabling the rule in “protect” mode to ensure legitimate traffic is not inadvertently blocked.

Manual Log Review

While a manual log review of firewall and IDS/IPS logs is very difficult, it is not impossible. The trick is to filter out the known benign log entries, leaving the log entries that need further scrutiny. A common error made by entities is working in reverse by developing filters for known traffic events that need to be responded to. As can be expected, this catches the known events but will miss the events previously not seen, thus failing the requirement.

The manual log review is best suited for low volume logs, typically generated by substation and generation plant electronic access control systems that do not readily support automated log

collection and analysis. Attempting to perform a manual review of a typical firewall or IDS/IPS log with the expectation of being able to “eyeball” those few entries signifying an intrusion is not realistic.

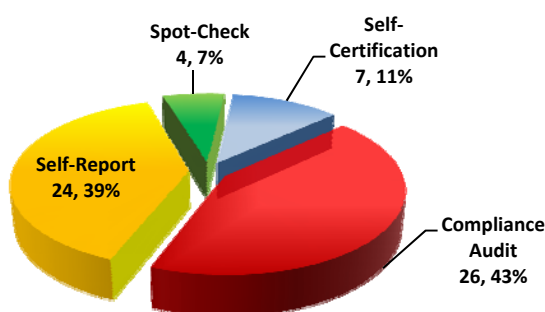
Manual Review by Sample

Paragraph 526 of FERC Order 706 states that the entity should manually review a sample of logs periodically to verify that the firewall rule sets, IDS/IPS signatures, and SIEM analysis triggers are appropriate and working properly. Entities should vary the sampled logs to permit every log to be reviewed over time and should establish a review periodicity appropriate to the number and size of the logs being collected. When performing the manual “sanity check,” filter out the known logs that the automated system is looking at to see if there is anything else that the automated systems either are unaware of or have missed due to a system mis-configuration.

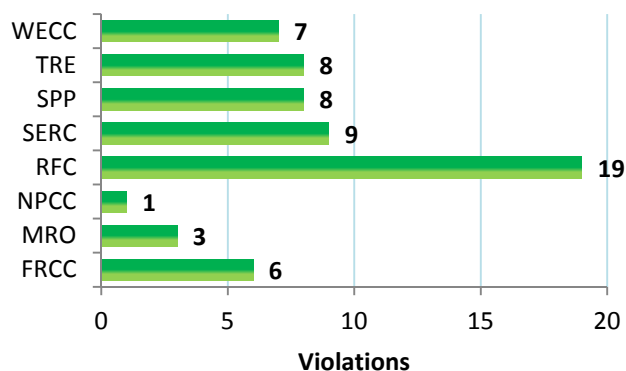
Detailed Requirement R4 Violation Information

CIP-005 Violations by Requirement	Violations	Percentage
R4 – Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually.	61	14.9%
Total	369	100%

R4 Violations by Method of Discovery



R4 Violations by Region



Violation Description Examples

- The entity failed to provide a list of required ports and services as required for the NERC standard and in Section Eight of its assessment program.
- Level of detail in cyber vulnerability assessment procedures was not adequate.
- The entity was in violation of CIP-005 R4 due to its failure to include a process for the discovery all access points to its electronic security perimeter in its 2009 vulnerability assessment.
- The entity did not complete its annual cyber vulnerability assessment within the required timeframe. The assessment was completed one month late due to delayed software upgrades.
- Entity provided evidence that a cyber vulnerability assessment of the management port of the access control device had been performed. Entity failed to review the entire access control device.

Case Notes

There are two Case Notes for R4: CIP-005-1 R4 and CIP-005-1 R4.

Suggested Enhancements

Ports and Services Review

Entities should have already established a baseline of required ports and services for each EACM, including firewalls, syslog servers, SIEM systems, VPN concentrators, Radius and TACACS+ servers, and Active Directory servers, as part of the compliance with CIP-005-3, R2. During the vulnerability assessment, entities should verify the ports and services enabled on an EACM system match those found in the baseline documentation. Additionally, entities need to review the ports permitted in the firewall rule sets (or other EACM Access Control Lists) against the list of ports required for communicating through the ESP access point to the protected Cyber Assets within the ESP. This is similar to the reviews required to sustain compliance with CIP-005-3, R2.2.

In order to demonstrate that a port or service is required for operations at an access point, an entity must be able to demonstrate why a port or service is required, not just that it is open or what the IANA Port Numbers list states. Also, audit teams will typically not accept vendor lists of required ports and services that do not state why a port or service is needed for operations.

CIP-005-3 R4.2 applies to ports and services permitted through the access point to the ESP, not just those active for management of the access control device. Entities should address their compliance with this in mind.

Discovery of electronic access points

A common error made by entities is performing a network scan within the ESP and believing that it alone constitutes a discovery of electronic access points. Unfortunately, that scan alone is insufficient. An electronic access point is essentially any Cyber Asset with a direct connection to a network segment within the ESP and a direct connection to a network segment outside the ESP. These types of systems are typically referred to as “dual-homed.” If IP Forwarding is enabled, the Cyber Asset essentially becomes a router into the ESP.

To properly perform a discovery of electronic access points, entities need to perform one or more of the following steps such that all network connectivity is identified:

1. Run “ipconfig /all” or equivalent on a Cyber Asset to identify every network interface enabled on that device. Identify the network segments the device is connected to and ensure none of those network segments are outside of the immediate ESP. Do not forget wireless and dial-up interfaces.
2. Physically inspect the Cyber Asset. Look for Ethernet, fiber optic, and modem cabling connected to the Cyber Asset and account for what networks the cables are connected to. Be cognizant of the fact that one cable can carry multiple VLANs of network traffic. If VLANs are configured, a physical cable inspection is insufficient without also considering the VLAN configuration in the connected communication device (e.g. a firewall or switch).

3. Scan all networks in the enterprise, not just the ESP-bounded networks, and correlate all discovered interfaces to the Cyber Assets connected through them.
4. Perform “war dialing” to identify any connected modems. Be aware that vendors occasionally install a dial-up (or high speed wide area network) connection for maintenance and support purposes and install the circuit as part of the support contract. Such dial-up circuits will not appear on the entity phone bill and will not be discoverable through war dialing techniques.

Review of default account, password, and network community string controls

As part of the entity’s cyber security policy, the security controls around default user accounts, passwords, and network community strings should be defined. These controls apply to the EACM systems. During the vulnerability assessment, entities should ensure the controls are still configured to the extent allowed by the device and that they are operating. For example, the user account and password requirements of CIP-007-3, R5 are applicable to the EACM systems through compliance with CIP-005-3, R1.5. Entities will need to ensure the initial password for a default account has been changed or the account disabled. Network community strings should be changed from the well-known default values. Passwords must comply where technically feasible with CIP-007-3, R5.3. If the device can be configured to partially or fully enforce these requirements, the entity should confirm that the configuration settings are still properly set.

Other assessments

Entities should also assess the EACM systems for compliance with some of the CIP-007-3 requirements that are applicable to the EACM system. This can include verification that any patches and updates have been applied, any anti-virus and other anti-malware is configured up-to-date, and operating properly, and that the system event logging is functioning properly.

Documentation

Entities are required to document the vulnerability assessment process. Entities can define a standard process or develop a customized process with each assessment. Entities will be expected to demonstrate that the vulnerability assessment followed the documented process.

Entities are also expected to document the results of the vulnerability assessment and develop an action plan to remediate any identified deficiencies. The action plan should be very detailed and should include measurable milestones that can be monitored and reported against. Entities should maintain the status and update it as it changes, and should report the remediation progress as directed by the entity policy on a regular basis. The action plan should be followed through within a defined time period.

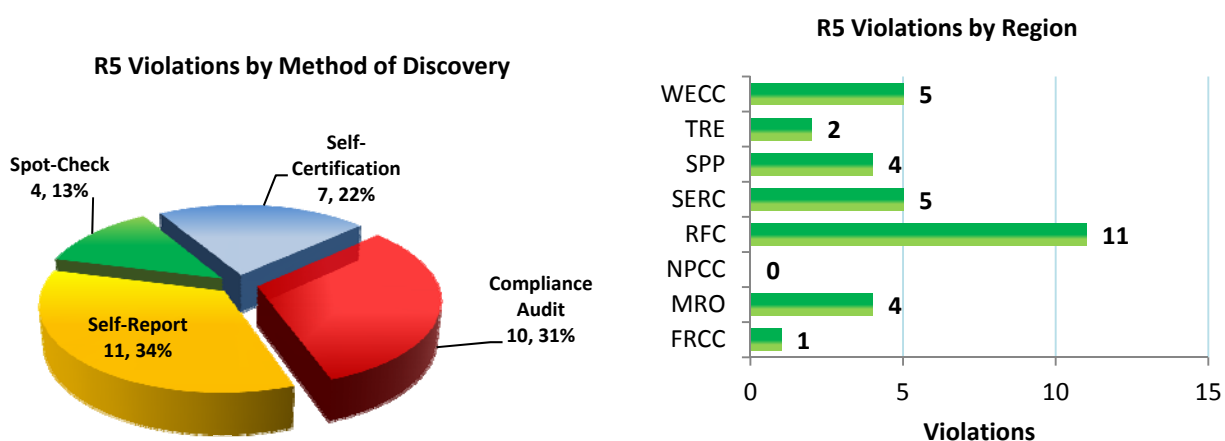
Cyber Vulnerability Assessment Additional Information

Entities should be aware that the cyber vulnerability assessment required by CIP-005-3 R4 is not the same cyber vulnerability assessment that is usually recognized by the security industry. CIP-005-3 R4 requires five things of the cyber vulnerability assessment: documentation of the cyber vulnerability assessment process, a ports and services review, ESP access point discovery, a review of account controls, and documentation of results including mitigation plans. Entities should note

that a “traditional” cyber vulnerability assessment with a tool such as Nessus or any of the commercial vulnerability scanners will probably not alone yield results an audit team can accept.

Detailed Requirement R5 Violation Information

CIP-005 Violations by Requirement	Violations	Percentage
R5 – Documentation Review and Maintenance —The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	32	9.1%
Total	369	100%



Violation Description Examples

- Entity failed to retain electronic access logs for at least 90 calendar days.
- The entity has no document to reflect current configurations and processes and therefore has not reviewed the documents and procedures referenced in Standard CIP-005-2 at least annually.
- R5.2: Entity evidence was insufficient to demonstrate that the entity updated the documentation to reflect the modification of the network or controls within 90 calendar days of the change. Entity restoration plan still includes back-up requirements for IBM-IPS devices that were removed more than 90 calendar days prior.

Case Notes

There are no Case Notes for R5.

Suggested Enhancements

Log retention

Logs must be retained for a minimum of 90 calendar days. In the event of a cyber security incident, the logs related to the event must be retained for at least three years. Entities will sometimes archive the logs on the same system that generated the logs. At a minimum, the archival logs should be backed up. A better practice is to copy the archival log files to a different

Cyber Asset for system separation and backup. A best practice, where entities are able, is to send the logs in real-time to a syslog server. This will inhibit a cyber intruder from deleting log records in an attempt to hide the attack.

Documentation updates and review

Entities must be able to demonstrate that required documentation was updated within 90 calendar days of the network or security controls modification. To do so, entities should maintain good records of any changes made, preferably through the CIP-003-3, R6 Change Control and Configuration processes. Entities should also maintain an auditable trail of the entity's documentation modifications with sufficient detail to demonstrate the documentation was updated as required.

Entities are also required to annually review all of the CIP-005-3 documentation, including the ESP, required ports and services, user authentication controls, appropriate use banners, electronic access monitoring and alerting processes, and the annual vulnerability assessment procedure. Entities need to maintain good records of the required documentation review, preferably for each document, as opposed to a blanket statement that may not be verifiable. While the standard does not specifically require the reviewed documents to be annually approved, it is a good practice to do so. Review and approval records can be maintained through a records management system or other work flow system that can assign and track actions, via the change log in the document, or a signed statement, either as part of the document or accompanying the document.

Conclusion

CIP-005 is a NERC Reliability Standard that is critical to the reliability of the BPS. As the violations continue to steadily accumulate, the ERO needs to provide feedback that will aid registered entities with compliance. Already in 2012 there have been 55 possible violations for CIP-005. It is advised that registered entities have an active and aggressive compliance monitoring program, a strong internal compliance program, and a solid culture of compliance within their organizations.

NERC looks forward to working with various industry and ERO working groups in developing the content for future Compliance Analysis Reports. The next Compliance Analysis Report will follow the same detailed structure as this report.

If you have any questions, please see below for contact information.

Contact Information

Mike Moon

Director of Compliance Operations
404.446.2567

Michael.Moon@nerc.net

Ryan Stewart

Engineer of Organization Registration,
Certification, and Compliance Monitoring
404.446.2569

Ryan.Stewart@nerc.net

Reliability Standards Audit Worksheet (RSAW) Development

Action

Information

Background

NERC is beginning to develop and update RSAWs by integrating the standard drafting team's (SDTs) intent, obtaining broader industry input and resolving compliance monitoring approaches. The objective of obtaining this input is to reduce any gap between the drafting team's intent for the standard and compliance expectations. Compliance and enforcement will continue to own the RSAW to ensure Compliance Enforcement Authorities (CEAs) appropriately and consistently monitor compliance; however, it is anticipated that this integration effort will, as RSAWs are modified, prevent spikes in the number of violations when standards become enforceable and prevent unnecessary violations for existing standards. This effort will also consolidate compliance guidance documents into one location as much as possible, where Compliance Enforcement Authorities (CEAs) and registered entities can easily access relevant information.

NERC is also beginning to incorporate the Risk-Based Compliance Monitoring Initiative concepts into the updated RSAWs by introducing formal auditing principles into compliance monitoring, including the assessment of internal controls. This widely accepted auditing practice¹ provides auditors an opportunity to assess whether a registered entity has control over its own compliance activities and the ability to use that assessment to determine the level of due diligence that will be required during the audit. Using this method, the auditor has the ability to monitor the entity's internal controls that are not subject to compliance and use the entity's evidence of compliance activities to verify the effectiveness of the internal controls. The updated RSAWs introduce these concepts with a discussion of the purpose for assessing internal controls during an audit and provide an opportunity for an entity to provide an auditor or CEA with its internal controls.

¹ Utilized in Generally Accepted Government Auditing Standards (GAGAS) and outlined in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) model; members of COSO include the American Accounting Association, American Institute of CPAs, Financial Executives International, The Association for Accountants and Financial Professionals in Business, and the Institute of Internal Auditors.

NERC is currently exploring several test options for RSAW development to cover various stages of current RSAWs:

- RSAWs for standards that are in development (Future Standards)
- RSAWs for:
 - Standards that have been approved by the NERC Board of Trustees (BOT) and are pending regulatory approval (FERC or Canadian Province)
 - Standards for which the BOT have approved an interpretation, either pending or post regulatory approval
 - Standards that have received the appropriate regulatory approval but are not yet enforceable
- RSAWs for existing standards

Each of the test options in process include varying levels of NERC committee involvement, Regional Entity feedback and industry participation to ensure the proper vetting of issues. Lessons learned from these test options will mold future methods of RSAW development.

Summary

Updating RSAWs is a key component of the ERO Risk Based Compliance Monitoring Initiative designed to:

- Allow for focus of resources on reliability issues
- Empower registered entities to be forward-looking and successful in their compliance activities

Updating RSAWs to be aligned with the SDTs intent and integrate formal audit principles into compliance monitoring, including assessing internal controls, is one of the major change elements of the Risk Based Compliance Monitoring Initiative. Other major change elements include assessing the frequency and scope of an entity's compliance monitoring based on the individual entity's potential impact on the reliability of the bulk power system (BPS) and the implementation of CEI Phase II, where discretion is applied in the field.

Materials:

1. Update on developing RSAWs, Slide presentation

Update on Enhanced Reliability Standard Audit Worksheets

This Project Supports 2012 NERC Corporate Goals One, Two and Four.

NERC is enhancing Reliability Standard Audit Worksheets (RSAW) by integrating the standard drafting team's (SDTs) intent, obtaining broader industry input and resolving compliance monitoring approaches. The objective of obtaining this input is to reduce any gap between the drafting team's intent for the standard and compliance expectations. Compliance and enforcement will continue to own the RSAW to ensure Compliance Enforcement Authorities (CEAs) appropriately and consistently monitor compliance; however, it is NERC's vision that this integration effort will, as RSAWs are modified, prevent spikes in the number of violations when standards become enforceable and prevent unnecessary violations for existing standards. Further, this effort will consolidate compliance guidance documents into one location, where CEAs and registered entities can easily access all relevant information.

NERC is exploring several options, which are listed below, to obtain the SDTs and industry perspective early in the process. These options include participation from NERC committees, industry trade groups and obtaining industry-wide comments. Due to the varying nature of the standards in which the RSAWs are going to be developed, more than one process may be necessary to ensure that the RSAWs are vetted with the appropriate industry members.

The RSAW appears to be a logical location for consolidating compliance information. RSAWs are designed for audit preparation and evidence verification, and therefore provide a single place for CEAs and registered entities to access relevant information. Such guidance that is being considered for inclusion is the SDTs intent, measures, data retention information, and other guidance from Compliance Application Notices (CANs).

NERC is also beginning to incorporate the Risk-Based Compliance Monitoring Initiative concepts into the updated RSAWs by introducing formal auditing principles¹ into compliance monitoring, including the assessment of internal controls. This widely accepted auditing practice provides auditors an opportunity to assess whether a registered entity has control over its own compliance activities and the ability to use that assessment to determine the level of due diligence that will be required during the audit. Using this method, the auditor has the ability to monitor the entity's internal controls that are not subject to compliance and use the entity's evidence of compliance activities to verify the effectiveness of the internal controls. The updated RSAWs introduce these concepts with a discussion of the purpose for assessing internal controls during an audit and provide an opportunity for an entity to provide an auditor or CEA with its internal controls.

¹ Utilized in Generally Accepted Government Auditing Standards (GAGAS) and outlined in the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) model; members of COSO include the American Accounting Association, American Institute of CPAs, Financial Executives International, The Association for Accountants and Financial Professionals in Business, and the Institute of Internal Auditors.

As a forward goal, additional information may be included to provide information regarding where a CEA is to apply discretion and professional judgment.

There are three categories of Reliability Standards to consider for RSAW development:

- Category 1: Future Standards
- Category 2: Revising Standards
 - Board of Trustees approved, pending regulatory approval
 - Board of Trustees approved interpretations
 - FERC and Canadian Provincial approval, not yet enforceable
- Category 3: Existing Standards

Under these categories, several development options are being considered:

- Category 1: Developing an RSAW in conjunction with a new Standard Project
 - Concept is currently being vetted through NERC committees and the Member Representatives Committee
- Category 2:
 - FAC-003-2 – sent to trade group (Transmission Forum) for technical feedback
 - COM-002-2a – sent to targeted NERC committees (Operating Committee and Compliance Certification and Committee) for technical feedback; has been posted for industry comment with comments due on April 30
 - PER-005-1 – initiated by Personnel Subcommittee, then sent to SDT for development, was reviewed by NERC standing committees (Operating Committee, Planning Committee, Critical Infrastructure Protection Committee), CCC and Standards Committee); has been posted for industry comment with comments due on April 30
- No RSAWs for existing standards have begun development at this time; several standards are under consideration.

Quarterly Statistics

Action

None

Background

NERC staff will present its regular quarterly report to the Committee and stakeholders on compliance statistics to fulfill the Committee's mandate obligations.

NERC is also working closely with the Regional Entities (REs) to develop a more consistent set of enforcement metrics. NERC and the REs have recently completed a review of the enforcement metrics used by all eight REs and NERC to establish a common understanding of what is being demonstrated through each particular metric. Future efforts will focus on identifying a finite set of metrics that measure the performance (timeliness, quality, effectiveness) of key Compliance Enforcement Authority (CEA) monitoring and enforcement activities that can be produced regularly, consistently, accurately, and with minimal resources for the individual regions and ERO Enterprise.

Among the metric concepts being considered are:

- Overall caseload index that quantifies the time it would take to clear violations in inventory based upon historical processing rates.
- Violations in inventory trending over time.
- Violation heat map illustrating total violations in inventory grouped by composite violation severity/risk level and correlated to actual processing times.
- Violation aging chart.
- Violation mitigation plan aging and status chart.