

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Compliance Monitoring and Enforcement Program 2012 Implementation Plan

Version 1.2

NOTE:

CMEP Implementation Plan and the 2012 Actively
Monitored Reliability Standards List are posted at:

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

December 14, 2011

to ensure
the reliability of the
bulk power system

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

Table of Contents

ERO Compliance Monitoring and Enforcement Program	1
Introduction	3
Risk-Based Compliance Monitoring Approach	5
2012 Implementation Plan Development Methodology	7
ERO High-Risk Priorities	7
FERC Order and Guidance	7
Violation Trend History	8
AML and Implementation Plan Input	11
Future Considerations	12
Three-Tiered Compliance Approach	12
Three-Tiered Approach to Requirements Specification	12
Three-Tiered Approach to Audit Scope Determination.....	13
Reliability Standards Subject to 2012 CMEP Implementation	16
High-Risk Priority Standards List.....	16
High-Risk Priority Standards and Tier 1 Requirements	17
BAL – Resource and Demand Balancing	17
CIP – Critical Infrastructure Protection	17
COM – Communications	17
EOP – Emergency Preparedness and Operations	17
FAC – Facilities Design, Connections, and Maintenance	18
IRO – Interconnection Reliability Operations and Coordination	18
MOD – Modeling, Data, and Analysis	19
NUC – Nuclear	19
PER – Personnel Performance, Training, and Qualifications	19
PRC – Protection and Control.....	19
TOP – Transmission Operations.....	20
TPL – Transmission Planning.....	20
CMEP Discovery Methods.....	22
Compliance Audits.....	22
Audit Focus or Scope.....	23
CIP Reliability Standards Compliance Audits.....	24
2012 Compliance Audit Schedule	24
Compliance Audit Reports.....	25
Compliance Tools	26
Mitigation Plans	26
Self-Certification.....	27
CIP-002-3 through CIP-009-3 Reliability Standards.....	27
Spot Checks	27

Table of Contents

CIP Reliability Standards.....	28
Periodic Data Submittals.....	28
Self-Reporting.....	28
Exception-Reporting.....	28
Reporting Credit	28
Complaint.....	29
Compliance Investigations.....	29
ERO Compliance Monitoring and Enforcement Program Organization.....	30
Compliance Enforcement	31
Program Scope and Functional Description.....	31
2012 Goals and Deliverables	31
Key CMEP Activities and Initiatives	34
CMEP Transparency Elements	34
Compliance Operations and REs Communications	35
Seminars and Workshops.....	35
Transparency Communications	35
Compliance Application Notices	36
Compliance Analysis Reports.....	38
Training.....	38
Compliance Auditors	38
Compliance Investigative (CI) Staff	38
Mitigation Plans	39
Non-Confirmed Violations Without Submitted Mitigation Plans	39
Registration and Certification	39
Multi-Regional Registered Entities (MRRE).....	39
Joint Registration Organization and Coordinated Functional Registration	40
Results of Abrupt or Forced Registration Changes	40
The Compliance Enforcement Initiative	41
Events Analysis Interface with Compliance	43
Regional Entities CMEP Implementation Plans.....	44
Conclusion	45
Appendix 1 – 2012 ERO High-Risk Priorities with High Value Associated Reliability Standards	47
Appendix 2 – 2012 Actively Monitored List (AML) Analysis	52
Appendix 3 – 2012 Regional Entity Request to Defer or Reduce the Scope of a Compliance Audit..	55
Appendix 4 – 2012 CMEP Implementation Plan Survey.....	57
Appendix 5 – Events Analysis Process Appendix G - Compliance Assessment Template	59

ERO Compliance Monitoring and Enforcement Program

Reliability and accountability are basic tenets of the Compliance Monitoring and Enforcement Program (CMEP). The objective of the North American Electric Reliability Corporation (NERC) and the Regional Entities is to achieve the highest possible level of reliability for the Bulk Power System (BPS). NERC, as the FERC-certified Electric Reliability Organization (ERO), together with the Regional Entities, is accountable to government regulators and industry stakeholders. The CMEP is critically important in supporting reliability and accountability, since effective compliance is a necessary, yet insufficient, activity for assuring the highest levels of reliability. The CMEP covers not only monitoring and enforcement activities, but also education, training and informational activities designed to assist the industry in achieving and sustaining effective compliance and enhanced reliability. The CMEP also complements other critical ERO activities aimed at improving reliability such as: facilitating the industry in the development and improvement of Reliability Standards, providing reliability assessments, and identifying lessons learned from events analysis that can assist the industry in enhancing reliability. There is clear ERO and industry accountability for the development of Reliability Standards in accordance with the 2005 Federal Power Act¹ and FERC Order No. 672², which duly recognize the collective expertise, experience and judgment needed to develop and improve Reliability Standards. NERC continues to refine and improve the annual CMEP and Actively Monitored List (AML) by focusing its efforts and resources on those areas that pose the greatest risk to reliability of the BPS.

As a reminder to all Registered Entities, NERC Rules of Procedure (RoP)³ state that all Bulk Power System users, owners, and operators are required to comply with all applicable ERO governmental authority-approved Reliability Standards at all times. Regional Reliability Standards and regional variances approved by NERC and the applicable ERO governmental authority are enforceable and apply to all Registered Entities responsible for meeting those Reliability Standards within the Regional Entity boundaries, whether or not the BPS user, owner, or operator is a member of the Regional Entity.

The CMEP is developed under Section 215(c) of the Federal Power Act⁴ to establish and enforce Reliability Standards for the BPS, subject to review by FERC and in general accordance with the “Principles for an Electric Reliability Organization that can Function

¹ Section 215(d)(2) of the Federal Power Act located at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6enr.txt.pdf

² *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, 114 FERC ¶ 61, 104 (2006) at P 324 located at http://www.nerc.com/files/final_rule_reliability_Order_672.pdf.

³ See Rules of Procedure, Section 401.2 at <http://www.nerc.com/page.php?cid=1|8|169>.

⁴ *Federal Power Act, 16 U.S.C. 824o. a.3 (2005)*. Located at http://www.nerc.com/fileUploads/File/AboutNERC/HR6_Electricity_Title.pdf

on an International Basis.”⁵ The CMEP is designed to improve reliability through the effective and efficient enforcement of Reliability Standards.

FERC Order No. 672 provides the framework for the ERO and its corresponding certification process. On July 20, 2006, FERC certified NERC as the ERO⁶. 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 recertified NERC as the ERO⁷ following the three-year assessment.

To help fulfill its responsibilities under its rules filed with regulatory authorities, NERC, as the international ERO, has delegated authority to qualified Regional Entities to monitor and enforce compliance with Reliability Standards by users, owners, and operators of the BPS. This delegation is governed by Regional Delegation Agreements (RDA) that have been approved by the appropriate regulatory authorities. NERC and these Regional Entities are responsible for carrying out the CMEP. Each Regional Entity submits its regional CMEP Implementation Plan to NERC for approval based on the requirements of this document.

NERC and the Regional Entities recognize that there are important reliability matters that require prompt communication to industry. NERC has used the Alerts/Advisory⁸ process to rapidly inform the industry of such matters. The Implementation Plan strongly encourages the applicable Registered Entities to proactively address such communications as a way of demonstrating good utility practice and a strong culture of compliance and reliability excellence.

⁵ Bilateral Electric Reliability Oversight Group, August 3, 2005 (the “Bilateral Principles”).

⁶ ERO Certification Order at P 3.

⁷ *North American Electric Reliability Corporation, Reliability Standards Development and NERC and Regional Entity Enforcement*, “Order on the Electric Reliability Organization’s Three-Year Performance Assessment,” 132 FERC ¶ 61,217 (2010 at P 1.

⁸ See Events Analysis: Alerts at <http://www.nerc.com/page.php?cid=5|63>.

Introduction

The ERO CMEP Implementation Plan is the annual operating plan for compliance monitoring and enforcement activities to ensure that NERC, as the international ERO, and the Regional Entities fulfill their responsibilities under legislation in the United States and other applicable obligations in jurisdictions in Canada and Mexico⁹.

Currently, Reliability Standards are mandatory and enforceable in the U.S. and the Canadian provinces of British Columbia¹⁰, Ontario¹¹, New Brunswick¹², and Saskatchewan¹³. The Canadian province of Alberta¹⁴ has adopted some of the Reliability Standards and is in the process of reviewing others. The legislative framework to make Reliability Standards mandatory and enforceable exists in Manitoba¹⁵, Nova Scotia¹⁶, and Quebec¹⁷. In Nova Scotia, the Reliability Standards are pending the approval of the Nova Scotia Utility and Review Board. The National Energy Board of Canada¹⁸ is in the process of making Reliability Standards mandatory and enforceable for international power lines.

The compliance monitoring and enforcement activities are carried out by NERC and the eight Regional Entities based on the regulatory authority-approved uniform CMEP¹⁹, the NERC RoP²⁰, the respective RDA²¹ with the eight Regional Entities, and other agreements including Memoranda of Understanding with the Canadian provinces. This plan outlines the implementation requirements to be followed by NERC and the eight Regional Entities. Each Regional Entity submits its 2012 Implementation Plan by November 1, 2011 to NERC. NERC is responsible for approving the Regional Entity Implementation Plans.²²

The 2012 Implementation Plan includes a set of Reliability Standards that were selected based upon ERO-identified high-risk priorities and a three-tiered approach to compliance auditing. The implementation plan also requires Regional Entities to consider a registered entity's compliance history when determining the scope of compliance monitoring activities. The objectives of the Implementation Plan are to:

- Promote the reliability of the BPS through rigorous compliance monitoring and enforcement activities.

⁹ http://www.cre.gob.mx/pagina_a.aspx?id=23

¹⁰ <http://www.nerc.com/files/British-Columbia112706.pdf>

¹¹ http://www.nerc.com/files/MOU_between_IESO_NERC_NPCC_02052010.pdf

¹² http://www.nerc.com/files/MOU_NewBrunswick-10032008.pdf

¹³ http://www.nerc.com/files/SaskPower_MOU_020309.pdf

¹⁴ http://www.nerc.com/files/NERC-WECC-AESO_MOU_Executed%20Version_071510.pdf

¹⁵ http://www.nerc.com/files/INTERIM_MANITOBA_AGREEMENT.pdf

¹⁶ http://www.nerc.com/files/NSPI_NERC_NPCC_MOU_executed_20100511.pdf

¹⁷ http://www.nerc.com/files/NERC-Regie-NPCC_Agreement_20090508EN_signed.pdf

¹⁸ <http://www.nerc.com/files/NEB-NERCMOU091406.pdf>

¹⁹ http://www.nerc.com/files/Appendix4C_Uniform_CMEP_20110101.pdf

²⁰ http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20110412.pdf

²¹ <http://www.nerc.com/page.php?cid=1%7C9%7C119%7C181>

²² See Appendix 4C of the NERC RoP at Section 4.2: <http://www.nerc.com/page.php?cid=1|8|169>

- Facilitate improved consistency of compliance activities throughout North America.
- Monitor all regulatory authority approved Reliability Standards by using the eight CMEP compliance monitoring methods.
- Use risk-based and performance-based criteria for determining the scope for compliance audits.
- Allow flexibility for the ERO and Regional Entities to investigate trends that may pose a near term risk to reliability either across the North American BPS, across an Interconnection or within a Regional Entity boundary.
- Improve the compliance program by analyzing the compliance monitoring experience across North America and implementing necessary improvements.

Risk-Based Compliance Monitoring Approach

The premise of risk-based compliance monitoring is that the amount of scrutiny a registered entity receives in terms of compliance monitoring will be directly commensurate with the risk it poses to the reliability of the BPS. Compliance monitoring encompasses a range of activities, including spot checks, self certifications, audits, and personal correspondence to an entity from the ERO. For entities that do not pose a significant reliability risk, the activities specifically prescribed in this Implementation Plan may suffice. For entities that do pose a significant risk to reliability, it will be necessary for those entities to undergo additional compliance monitoring such as additional focused spot checks, a greater number of self certifications, or broader and deeper audits of greater frequency, etc.

Registered Entities are responsible for compliance with all regulatory approved Reliability Standards and Requirements in effect per their registered function at all times, regardless of what is specified in the AML.

One of the key components to an effective risk-based audit approach is the incorporation of performance-based auditing. Performance audits, according to the United States Government Accountability Office²³, are defined as engagements that provide assurance or conclusions based on an evaluation of sufficient, appropriate evidence against stated criteria, such as specific requirements, measures, or defined business practices. 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 are being implemented, rather than relying solely on documentation.

To assist the Regional Entities in determining how much risk an entity poses to reliability, a number of aspects have been identified that point to activities, behaviors, and qualities that warrant additional concern prompting an enhanced application of compliance monitoring. Specifically, these aspects include the Technical and Risk Profile of an entity, Reliability Performance Metrics, an entity's Internal Compliance Program, Compliance and Enforcement Metrics and Status, and Regional Entity Qualitative Assessment, which are concepts described in generally accepted government auditing standards (GAGAS)²⁴. These five aspects are described below:

- **Technical and Risk Profile:** This profile details the technical components of the Registered Entity. It highlights various aspects of the company's structure and identifies key information that is relative to its risk. Such components include

²³ See United States Government Accountability Office – Government Auditing Standards (GAGAS) at Chapter 1: Use and Application of GAGAS at Section 1.25 <http://www.gao.gov/new.items/d07731g.pdf>.

²⁴ See GAGAS at Chapter 7: Field Work Standards for Performance Audits <http://www.gao.gov/new.items/d07731g.pdf>

MW capacities, registration information, points of interconnection, and affiliated companies.

- **Reliability Performance Metrics (Trends):** Metrics provide a quantitative approach for measuring a registered entity's performance. Consistent metrics yield a baseline to measure performance as well as compare performance to previous years.
- **Internal Compliance Program:** The strength of a registered entity's internal compliance program evidences its activities to self-monitor reliability and compliance through internal controls, corrective action programs and a culture of compliance. An assessment of a registered entity's internal compliance program includes an evaluation of how the entity addresses the standard FERC 13 questions and the additional FERC 1b compliance criteria, and outlines areas for improvement in the internal compliance program.
- **Compliance and Enforcement Metrics and Status:** These metrics detail the violation history and any open enforcement actions of the registered entity, including consideration of the facts and circumstances surrounding the violations. The evaluation includes consideration of the methods of discovery, with specific focus on repeat violations, the status of any open mitigation plans, and compliance improvements over time.
- **Regional Entity Qualitative Assessment:** This area provides an opportunity for the Regional Entities to include qualitative assessment and regional expertise for what the entity is doing well and areas for improvement.

NERC and the Regional Entities will work together to develop an Entity Risk Profile Assessment template for use across the entire ERO before the end of 2011. When complete, this template will be publically posted on NERC's website for the benefit of both the Regional Entities and registered entities. For registered entities, the template may prove valuable for conducting critical self-assessments in preparation of compliance monitoring actions and other times. Also, the template will be invaluable for the Regions in order to scope audits appropriately.

It must be emphasized that registered entities are responsible for compliance with all regulatory approved Reliability Standards and Requirements in effect per their registered function at all times, regardless of what a registered entity's risk profile may indicate. Regional Entities have the authority and responsibility to expand the scope of an audit, spot check, or any other compliance monitoring process if they consider it necessary when evaluating the compliance of a registered entity.

2012 Implementation Plan Development Methodology

As part of an overall compliance plan, NERC developed the AML of Reliability Standards for 2012 based on the methodology outlined in this section. This framework is a continuation of the initial development process for the 2011 Implementation Plan.

The 2012 Implementation Plan is designed to realize risk-based approaches for ERO programs, priorities and initiatives that meet reliability goals and improve efficiencies. Achieving these goals will be accomplished through the development, maintenance, and implementation of a list of the highest priority Reliability Standards. The Reliability Standards and associated Requirements populating this list will be determined through an annual 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
- Future Considerations

ERO High-Risk Priorities

The purpose of identifying and using a set of priorities is to move away from focusing on processes for “administrative and documentation-related violations that have no effect on bulk power system reliability,” as the Edison Electric Institute (EEI) has stated²⁵. Instead, the focus is on those Reliability Standards, and more specifically those Requirements within the Reliability Standards, that are most critical to the reliability of the BPS as determined by a set of risk-based criteria. The priorities and correlated Reliability Standards are explained in further detail in *Appendix 1 - 2012 ERO High-Risk Priorities with High Value Associated Reliability Standards*. NERC and the Regional Entities considered these priorities and identified a number of Reliability Standards that apply to each criteria. Many of these Reliability Standards apply to multiple priorities, bolstering their importance and reason for inclusion into the AML.

FERC Order and Guidance

FERC Order No. 729 states that “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. The Commission clarifies that these audits are not intended to address the competitive effects of these MOD Reliability Standards. Instead, the audit should review each component of

²⁵ http://www.nerc.com/docs/bot/finance/2010BPB_EEI_Draft2comments.pdf

available transfer or flowgate capability, including the transmission service provider’s calculation of capacity benefit margin and transmission reliability margin, for transparency and verifiability to ensure compliance with the MOD Reliability Standards.”²⁶

The Reliability Standards associated with this order that will be integrated into the 2012 Implementation Plan are MOD-001, MOD-004, and MOD-008.

Violation Trend History

An analysis of the compliance history of Reliability Standards is only one aspect for determining the risk-based compliance approach, and provides insight into which Reliability Standards have proven most challenging for registered entities. Reliability Standards that are understood by registered entities appear to result in more possible violations through the self-report monitoring method. Reliability Standards that are not understood by registered entities, or are complicated, appear to result in more possible violations through the audit and spot check monitoring methods. Through the identification and inclusion of these Reliability Standards in the annual compliance plan, registered entities will have the ability to learn through personal experience, regional workshops, and other outreach programs and resources on how best to improve their compliance programs. Improved compliance programs will result not only in enhanced compliance for these Reliability Standards in particular, but also for all remaining Reliability Standards, through the growth of compliance processes and systems.

A collection of violation statistics results for all Reliability Standards, displayed for all regions as referenced by the ERO and according to each Interconnection, can be seen according to the near term and since June 18, 2007 in Tables 1 and 2 respectively.

Table 1: Top 10 Violation Statistics for the near term in all Regions and by Interconnection for all Reliability Standards.

Rolling 12 Month (3.28.2010 to 3.28.2011)								
	NERC		Eastern Interconnection		Western Interconnection		ERCOT Interconnection	
	Standard	Violations	Standard	Violations	Standard	Violations	Standard	Violations
1	CIP-007	297	CIP-007	187	CIP-007	84	PRC-005	29
2	PRC-005	199	CIP-004	128	CIP-004	55	CIP-007	26
3	CIP-004	192	PRC-005	121	CIP-006	53	CIP-001	19
4	CIP-006	133	CIP-005	83	PRC-005	49	CIP-004	9
5	CIP-005	131	CIP-006	72	CIP-003	43	CIP-006	8
6	CIP-003	107	CIP-001	62	CIP-005	40	CIP-005	8
7	CIP-002	90	CIP-003	61	CIP-002	36	IRO-001	8
8	CIP-001	89	VAR-002	54	CIP-009	25	VAR-002	7
9	VAR-002	77	CIP-002	52	VAR-002	16	PRC-001	6
10	CIP-009	59	FAC-008	36	CIP-008	9	TPL-002	6

²⁶ 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 (2009) at P 106.

Table 2: Top 10 Violation Statistics for all time in all Regions and by Interconnection for all Reliability Standards.

All Time								
	NERC		Eastern Interconnection		Western Interconnection		ERCOT Interconnection	
	Standard	Violations	Standard	Violations	Standard	Violations	Standard	Violations
1	PRC-005	678	PRC-005	425	PRC-005	214	PRC-005	39
2	CIP-001	442	CIP-004	260	CIP-001	184	CIP-001	30
3	CIP-004	390	CIP-007	232	CIP-004	119	CIP-007	26
4	CIP-007	372	CIP-001	228	CIP-007	114	FAC-008	19
5	CIP-006	178	FAC-008	123	TOP-002	80	IRO-001	12
6	FAC-008	171	CIP-006	109	EOP-005	72	CIP-004	11
7	VAR-002	158	CIP-005	103	CIP-003	64	PRC-008	10
8	CIP-005	156	VAR-002	95	CIP-006	61	VAR-002	10
9	CIP-003	152	FAC-009	94	PER-002	55	FAC-009	9
10	CIP-002	135	CIP-002	86	VAR-002	53	CIP-006	8

With the significant presence of FERC Order No. 706²⁷ (CIP) Reliability Standards among violations, especially in the near term, it becomes difficult to gauge how the FERC Order No. 693²⁸ Reliability Standards rank in terms of violations. Removing the CIP Reliability Standards from this analysis, the violation statistics for 693 Reliability Standards in the near term and for all time can be seen in Tables 3 and 4 respectively.

Table 3: Top 10 Violation Statistics for the near term in all Regions and by Interconnection for FERC Order No. 693 Reliability Standards.

Rolling 12 Month (3.28.2010 to 3.28.2011) w/o CIP								
	NERC		Eastern Interconnection		Western Interconnection		ERCOT Interconnection	
	Standard	Violations	Standard	Violations	Standard	Violations	Standard	Violations
1	PRC-005	199	PRC-005	121	PRC-005	49	PRC-005	29
2	VAR-002	77	VAR-002	54	VAR-002	16	IRO-001	8
3	FAC-008	42	FAC-008	36	PRC-008	9	VAR-002	7
4	PRC-008	36	TOP-002	30	BAL-004	5	PRC-001	6
5	FAC-009	32	FAC-009	25	EOP-005	5	TPL-002	6
6	TOP-002	32	PRC-008	23	IRO-STD	4	FAC-009	5
7	COM-002	24	COM-002	20	PER-002	4	TOP-001	5
8	PER-002	21	FAC-001	17	PRC-023	4	PRC-008	4
9	PRC-001	21	PER-002	17	COM-002	3	PRC-004	4
10	FAC-001	20	FAC-003	16	FAC-001	3	FAC-008	4

²⁷ *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 (2008) (Order No. 706).

²⁸ *Mandatory Reliability Standards for the Bulk-Power System*, 72 FR 16,416 (Apr. 4, 2007), FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693). NERC realizes each Canadian province has separate Memoranda of Understanding and the use of 693 and 706 in this document for referencing CIP and non-CIP standards.

Table 4: Top 10 Violation Statistics for all time in all Regions and by Interconnection for FERC Order No. 693 Reliability Standards.

All Time w/o CIP								
	NERC		Eastern Interconnection		Western Interconnection		ERCOT Interconnection	
	Standard	Violations	Standard	Violations	Standard	Violations	Standard	Violations
1	PRC-005	678	PRC-005	425	PRC-005	214	PRC-005	39
2	FAC-008	171	FAC-008	123	TOP-002	80	FAC-008	19
3	VAR-002	158	VAR-002	95	EOP-005	72	IRO-001	12
4	TOP-002	133	FAC-009	94	VAR-002	53	PRC-008	10
5	EOP-005	129	EOP-005	57	EOP-001	50	VAR-002	10
6	FAC-009	127	FAC-003	56	FAC-001	47	FAC-009	9
7	PRC-008	104	FAC-001	53	PRC-008	46	PRC-001	6
8	FAC-001	100	TOP-002	52	VAR-001	44	TOP-001	6
9	PER-002	98	PRC-008	48	TPL-002	35	TPL-002	6
10	EOP-001	84	PER-002	43	COM-001	31	IRO-004	4

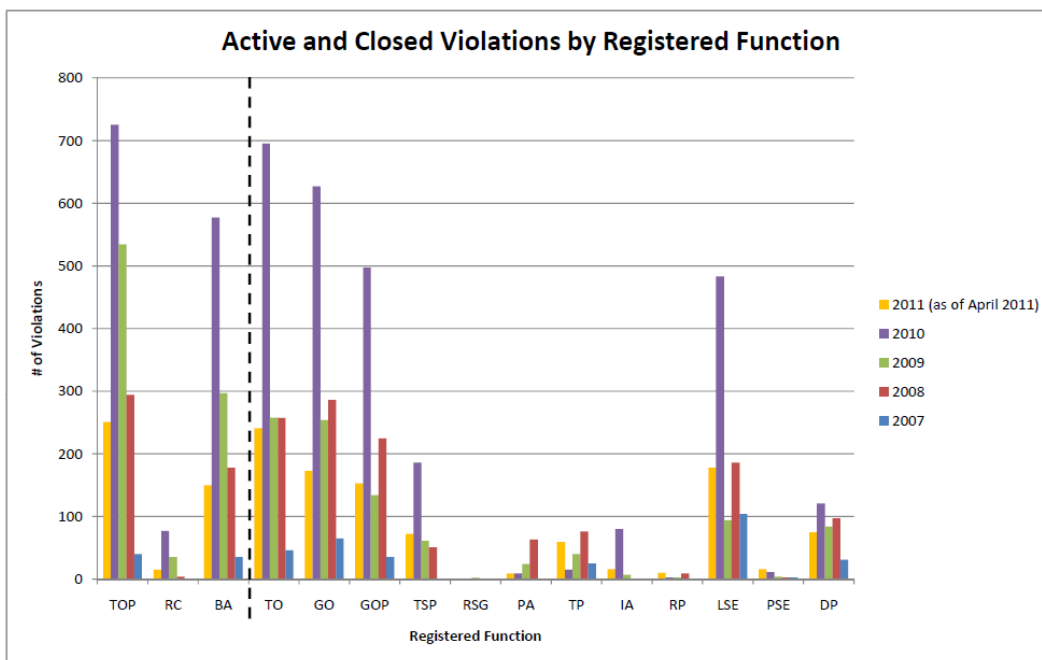


Figure 1: Active and Closed violation summary history per function since 2007.

As a final perspective on violations for recent years, Figure 1 displays the number of active and closed violations attributed to the various registered functions since June 18, 2007. The violations for each function are not necessarily specific or unique violations to each function alone in all cases. Rather, in many cases, a single violation will be applicable to more than one function, resulting in each of the applicable functions reflecting this one violation.

Risk-based compliance includes high-impact violations as well as low-impact violations that are widespread enough to, as an aggregate, represent a high impact to reliability. Thus, violation history is an important tool for assessing which Reliability Standards and, in turn, which functions have proven to be most difficult for compliance and require more attention during audits.

AML and Implementation Plan Input

All eight Regional Entities provided valuable input into the development of the 2012 AML and Implementation Plan. Input was received from members of the ERO Compliance and Enforcement Management Group (ECEMG), the Compliance Monitoring Processes Working Group (CMPWG), and various Regional Entity compliance and enforcement staff.

In addition to the input provided by the Regional Entities, several NERC departments provided insight in terms of the relationship of Reliability Standards to ERO High-Risk Priorities, supplementary information from these groups has been provided in order to help further refine the list of High-Risk Priority Standards. Specifically, the departments that contributed to the 2012 Implementation Plan include Compliance Operations, Critical Infrastructure Protection, Enforcement, Events Analysis and Investigations, Legal, Resource Assessments and Performance Analysis, and Standards.

The Reliability Assessment and Performance Analysis department has completed an analysis in which a subset of Requirements with the highest impact to reliability has been identified according to a Standards/Statute Driven Index (SDI), which measures improvement in compliance with Reliability Standards, as part of a Reliability Metrics and Integrated Risk Assessment study²⁹. This subset consists of 26 Requirements and is found in Table 5. These Requirements have high Violation Risk Factors (VRFs) and the violations of these Requirements had severe Reliability Impact Statements (RIS), as determined by the Regional Entity.

Table 5: 26 Requirements considered by the Standards/Statute Index as part of Reliability Metrics and Integrated Risk Assessment

Standard	Req.	Standard	Req.	Standard	Req.	Standard	Req.	Standard	Req.
EOP-001-0	R1.	FAC-009-1	R1.	PER-002-0	R3.	PRC-005-1	R2.	TOP-004-2	R1.
EOP-003-1	R7.	IRO-005-2	R17.	PER-002-0	R4.	TOP-001-1	R3.	TOP-004-2	R2.
EOP-005-1	R6.	PER-001-0	R1.	PRC-004-1	R1.	TOP-001-1	R6.	TOP-006-1	R6.
EOP-008-0	R1.	PER-002-0	R1.	PRC-004-1	R2.	TOP-001-1	R7.	TOP-008-1	R2.
FAC-003-1	R1.	PER-002-0	R2.	PRC-005-1	R1.	TOP-002-2	R17.	VAR-001-1	R1.
FAC-003-1	R2.								

The Reliability Assessment and Performance Analysis group has also completed an analysis of the BPS transmission system through the Transmission Availability Data System (TADS). As shown in Figure 2, this analysis points to several causes for sustained outages experienced by North America’s transmission system. Keeping these outage causes in mind can be helpful in determining the priority of individual Requirements within already designated, high-risk priority Reliability Standards.

²⁹ http://www.nerc.com/docs/pc/rmwg/Integrated_Reliability_Index_WhitePaper_DRAFT.pdf

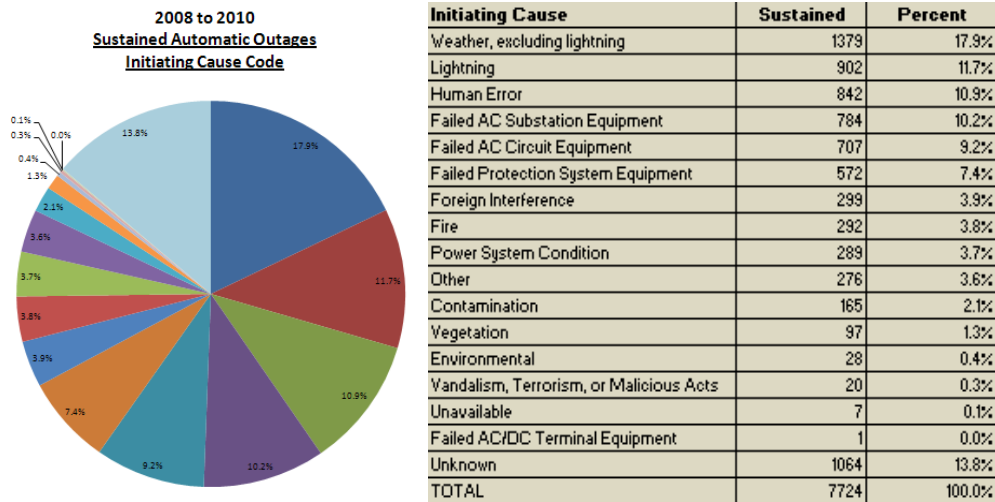


Figure 2: Initiating causes of sustained outages for the BPS from 2008 to 2010.

Future Considerations

Future considerations refer to those Reliability Standards that are not yet enforceable, but are implicated by the 2012 ERO high-risk priorities as referenced in Appendix 1. Thus, these suggested Reliability Standards provide guidance on what should immediately be considered for incorporation into the AML following FERC approval and given the current priorities. As indicated by the NERC standards group, the applicable Reliability Standards subject to future enforcement include EOP-005-2, PER-005-1, and PRC-004-2.

Three-Tiered Compliance Approach

Following the compilation of the complete list of highest priority Reliability Standards, the AML, being the minimum scope of compliance audits, will include a subset³⁰ of Requirements per the FERC-approved RoP. The Requirements identified for the 2012 AML by using a three-tiered approach are described below.

Three-Tiered Approach to Requirements Specification

After selecting a set of Reliability Standards based upon the priorities and criteria identified above, it is necessary to identify the specific Requirements within each of the Reliability Standards that most directly relate to the purpose of the standard itself in terms of its relationship to the identified ERO high-risk priorities and, ultimately, its support for the reliability of the BPS.

In accordance with the FERC-approved Rules of Procedure, the ERO has selected a subset of the Reliability Standards and Requirements to be actively monitored and audited in the ERO annual compliance program for 2012. The three-tiered approach for identifying the Requirements of the Actively Monitored List is described below. For

³⁰ See NERC RoP, Section 401.6.

further information regarding the Implementation Plan methodology, refer to *Appendix 1 – 2012 ERO High-Risk Priorities with High Value Associated Reliability Standards*.

Tier 1 Requirements are those that are the most critical to the purpose and intent of the standard of which they are a part. Additionally, the ability of a registered entity to demonstrate compliance with Tier 1 Requirements will provide guidance to audit teams on the necessity to investigate further and broaden an audit's scope in additional Requirements and/or Reliability Standards.

Tier 2 Requirements are also critical to the purpose of a standard, but less so than Tier 1 in that Tier 2 does not address the ERO high-risk priorities as does Tier 1. Tier 2 also does not pose as severe a risk as Tier 1. This is not to say that compliance with Tier 2 Requirements is not mandatory. Instead, Tier 2 Requirements represent an additional level of inquiry that must be undertaken when a registered entity does not display clear compliance with those most critical Requirements of Tier 1. In the process of this added level of investigation, it may become necessary to branch off into other Reliability Standards that were not identified as relating directly to an ERO priority.

Tier 3 Requirements are those that, while still being significant to BPS reliability, do not represent the purpose of a Reliability Standard directly or are not representative of ERO priorities. The exploration of an audit team into the compliance of a registered entity with Tier 3 Requirements will be initiated through links between identified deficiencies in Tier 1 and 2 Requirements and those of Tier 3.

Regional Entity audit teams are authorized and obligated to expand the scope of a compliance audit to include Tier 2 and Tier 3 Requirements and any other requirements they may deem necessary based on the results of the Registered Entity Profile Assessment or the audit team's collective professional judgment. Audit scope expansion can occur at any point during the process: from the initial review of the Registered Entity Profile Assessment through the close of the audit.

The implementation plan for 2012 will use Tier 1 Requirements as the AML of Reliability Standards. The basis for the requirements of the high-risk priority Reliability Standards in the Tier 1 classification is covered in the following section.

Three-Tiered Approach to Audit Scope Determination

The three-tiered approach is new for 2012. Tier 1 Requirements are identified in the 2012 AML and represent the minimum scope of compliance audits. The potential expansion of an audit into Tier 2 and Tier 3 Requirements will be determined by the Regional Entity based on the results of a risk-based compliance monitoring and entity profile assessment or as determined during the audit process. When a Regional Entity determines that an increased audit scope is necessary based on a risk-based compliance monitoring approach, then the Regional Entity shall notify the registered entity of the increased audit scope. This notification shall include the Reliability Standards and

Requirements that are included in the increased scope, as well as the justification for the increased scope. This notification shall be part of the audit notification package when increased scope is determined early enough in the process. When a Regional Entity determines that an increased audit scope is necessary after the notification package is sent, or while the audit team is on-site, then the Regional Entity shall notify the registered entity of the increased audit scope as soon as possible.

The audit scope for registered entities that are registered to perform identical “functions” will not always be identical across or within the Regional Entities. Registered entities will be advised of the audit scope when they receive the formal audit notice. Compliance information and data archived by the Regional Entity from the implementation of previous monitoring methods will be used 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. Regional Entities will determine the registered entity’s specific audit scope based upon the NERC Actively Monitored Reliability Standards List.

Regional Entities are authorized and obligated to implement the annual NERC Implementation Plan. Regional Entity staff may increase the scope of compliance activities related to the NERC program, as described above, but cannot reduce the scope of compliance activities without NERC consent. Where Regional Entities determine that a reduced scope is appropriate, the Regional Entity will submit the *Regional Entity Request to Defer or Reduce the Scope of a Compliance Audit*, which is located in Appendix 3 to the NERC Compliance Operations department at least 90 days prior to the audit for approval.

For Reliability Standards that are incorporated into a compliance audit as the result of a scope expansion, the registered entity that is subject to review of these additional Reliability Standards will not be expected to provide evidence outside of the audit period under review. Registered entities will not be expected to provide evidence outside of the current audit period for the purposes of demonstrating compliance with Reliability Standards unless that evidence is required in accordance with the processes and procedures of the registered entity. For example, a registered entity is expected to provide evidence outside of the current audit period for substantiating long range plans that are longer than an audit period, such as Protection System maintenance and testing intervals. For those Reliability Standards that do not involve long-range plans, an audit team will not be able to request information that is outside of the bounds of the current audit—either three or six years—nor can it identify possible non-compliance outside of this audit period. In other words, the completion of an audit closes one audit period and initiates another, excluding future audit teams from reviewing a registered entity’s compliance during past audit periods. This exclusion does not apply to ERO enforcement actions or investigations. Generally speaking, spot checks, data submittals, and self-certifications will not require evidence that precedes the current audit period. This exclusion does not apply to ERO enforcement, investigations, or events analysis. Generally speaking, spot checks, data submittals and self-certifications will not require evidence that precedes the current audit period.

The overall monitoring scope of the 2012 Implementation Plan and AML is based on Reliability Standards that are anticipated to be in effect on January 1 2012. To the extent new or revised Reliability Standards are adopted, approved by the regulatory authority or in effect during the course of 2012, NERC will work with the Regional Entities to determine whether the 2012 program needs to be amended.

All NERC Reliability Standards identified in the 2012 Implementation Plan are listed in the 2012 CMEP Actively Monitored Reliability Standard list posted on the NERC website at the following link: <http://www.nerc.com/commondocs.php?cd=3>

The 2012 Actively Monitored Reliability Standards list includes several worksheets. A description of each is listed below:

- **Summary Tabs:** Quick reference listings of the Reliability Standards and Requirements identified for compliance audits, self-certifications and spot checks required by NERC in 2012, and mandatory effective dates for Reliability Standards. These tabs are designed to give the user a quick reference of the Implementation Plan lists. There are also comparisons of the number of Reliability Standards and Requirements monitored in the 2007, 2008, 2009, 2010, and 2011 programs.
- **Requirements Detail Tab:** A detailed list of the Requirements included in the 2012 Implementation Plan.
- **Revision History:** The revision history that will allow users, owners and operators of the BPS to see all of the changes to the 2012 Actively Monitored Reliability Standards spreadsheets.

An analysis of the applicability of Tier 1 to the various registered functions is located in Appendix 2. Table 6 highlights some of this analysis and compares the 2012 AML to previous years.

Table 6: Requirements Analysis for the 2012 AML and those going back to 2007

Function	Requirements Analysis								
	Total Applicable Reqs as of 1/1/2012	2012 AML (All Reqs)	2012 AML (CIP only)	2012 AML (693 only)	2011	2010	2009	2008	2007
TOP	499	170	109	61	246	321	134	142	115
RC	397	136	109	27	203	299	97	131	76
BA	408	155	109	46	206	305	107	175	95
TO	369	134	107	27	222	271	70	86	86
GO	302	119	107	12	198	242	34	47	40
GOP	254	121	109	12	168	242	27	38	13
TSP	318	166	107	59	202	206	5	7	2
RSG	20	2	0	2	0	6	6	20	20
PA/PC	178	6	0	6	42	88	56	89	86
TP	143	13	0	13	49	83	51	86	86
IA	184	107	107	0	145	168	0	0	0
RP	22	3	0	3	3	0	0	0	0
LSE	267	123	109	14	157	214	12	26	13
PSE	11	1	0	1	1	3	3	4	3
DP	129	9	0	9	51	54	21	51	51
Avg Reqs	233	84	65	19	126	167	42	60	46

Reliability Standards Subject to 2012 CMEP Implementation

The regulatory authority-approved Reliability Standards and Requirements are monitored through at least one of the CMEP compliance monitoring methods. For the “audit” monitoring method, NERC and the Regional Entities have developed and implemented risk-based and performance-based criteria for determining the scope of the Reliability Standards to be reviewed during the conduct of the audit; risk-based and performance-based audits are discussed in *Chapter 3 - 2012 Implementation Plan Development Methodology*. In addition to these established priorities, other elements considered include FERC Orders and Guidance, compliance history, NERC departmental input, and future considerations utilizing a three-tiered approach. Audit scope is determined by factors that are associated with BPS issues across North America, across the respective Interconnection, and within a Regional Entity boundary, as well as specifics associated with a registered entity.

High-Risk Priority Standards List

Given the considerations of the ERO-identified high-risk priorities, as discussed in Appendix 1, which includes compliance history and violation trend analysis, the number of high priority Reliability Standards is 50, as shown in Table 7. From this group of Reliability Standards, it has been the primary task of Compliance Operations working with input from other groups within NERC to determine and rank the specific Requirements of each standard that best represent the core purpose of that standard to ensure the reliability of the BPS. With the further refined list of Requirements, a subset has been taken as the 2012 AML and will be monitored by the Regions during the year in accordance with the CMEP.

Table 7: High-Risk Priority Reliability Standards

BAL-002	CIP-009	FAC-001	MOD-004	PRC-011
BAL-003	COM-001	FAC-002	MOD-008	PRC-023
CIP-001	COM-002	FAC-003	NUC-001	TOP-001
CIP-002	EOP-001	FAC-008	PER-001	TOP-002
CIP-003	EOP-002	FAC-009	PER-002	TOP-003
CIP-004	EOP-003	IRO-002	PRC-001	TOP-004
CIP-005	EOP-004	IRO-004	PRC-004	TOP-006
CIP-006	EOP-005	IRO-005	PRC-005	TOP-008
CIP-007	EOP-006	IRO-006	PRC-007	TPL-003
CIP-008	EOP-008	MOD-001	PRC-008	TPL-004

High-Risk Priority Standards and Tier 1 Requirements

For each high priority standard identified in Table 7 above, only those Requirements that are recognized as Tier 1 Requirements will become part of the AML of Reliability Standards that must be examined during compliance audits. This section presents a synopsis of the details considered within each group of Reliability Standards to determine the Requirements that meet Tier 1 criteria. Refer to the 2012 AML to view the specific Requirements selected for each of the high-risk priority Reliability Standards.

BAL – Resource and Demand Balancing

BAL-002-0 and BAL-003-0.1b have been identified as high priority Reliability Standards. The performance aspect of BAL-002 is reviewed quarterly through periodic data submittals, but recent winter weather events have shown that contingency reserve is a critical issue, such that special attention should be given here. BAL-003-0.1b has been subject to spot checks in the past, but technical issues discovered through its enforcement have yet to be addressed. Until additional guidance is provided through interpretations, revisions, or otherwise, the Requirements of BAL-003 will be treated as Tier 2 Requirements.

CIP – Critical Infrastructure Protection

CIP-001-2a, CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3a, CIP-006-3, CIP-007-3, CIP-008-3, and CIP-009-3 have been identified as high priority standards. CIP-001 has an important role as BPS personnel become aware of and properly report sabotage events. Preparedness for reporting, as well as procedures to determine to whom reports should be issued, are critical in mitigating the occurrence of any such event. CIP-002 through CIP-009, or 706 Reliability Standards, are fundamental to the reliability of the BPS in terms of cyber security. Additionally, the CIP Reliability Standards represent eight of the Top 10 Reliability Standards violated over the past year and seven of the Top 10 for all time, indicating that registered entities are having difficulty with compliance issues. Several groups, including NERC, FERC, and the Regional Entities, have provided insight into the various Requirements in greatest support of the purpose of these Reliability Standards.

COM – Communications

COM-001-1.1 and COM-002-2 have been identified as high priority Reliability Standards. COM-001 details and mandates the adequacy of telecommunication facilities, thus supporting nearly every function, and is critical to normal and emergency operations. COM-002 has some similar coverage as COM-001, but goes above and beyond with three-part communication and a methodology for formulating directives. Also, COM-002 is the seventh-most-violated 693 standard for the past year as noted above in Table 3.

EOP – Emergency Preparedness and Operations

EOP-001-0, EOP-002-2.1, EOP-003-1, EOP-004-1, EOP-005-1, EOP-006-1, and EOP-008-0 have been identified as high priority Reliability Standards. EOP-001 is critical in

terms of Energy Emergency Alerts (EEAs), which were important for mitigating impacts from winter weather events taking place during early 2011. EOP-002 complements EOP-001 by assuring the performance of mitigating actions for the both the RC and the BA. EOP-003 designates load-shedding as a suitable action for maintaining the reliability of the BPS, but its action is implied in EOP-001, and therefore the Requirements of EOP-003 are not considered Tier 1 Requirements. EOP-004 is critical in terms of events analysis and helping with the process of mitigating future events, and it is vital that the disturbance reports do not stay within a region, but are shared with NERC for dissemination across North America. EOP-005 sets the foundation for system restoration if actions identified in other EOP Reliability Standards fail and the testing and confirmation of a blackstart capability process is engaged. EOP-006 ensures that the Reliability Coordinator takes the lead role in system restoration initiated through EOP-005, such that coordination in these efforts is not an oversight. EOP-008 accounts for loss of a primary control center and many Requirements not accounted for in any other standard, so this is vital to include.

FAC – Facilities Design, Connections, and Maintenance

FAC-001-0, FAC-002-0, FAC-003-1, FAC-008-1, and FAC-009-1 have been identified as high priority Reliability Standards. FAC-001 designates connections requirements for facilities, which is especially critical in terms of protection and construction of new facilities. With these facilities properly coordinated and accounted for, existing system performance will improve. FAC-002 expands on FAC-001 by requiring that assessments for facilities be undertaken and results coordinated. FAC-003 concerns vegetation management, which is a primary initiator of many events and points to the necessity of an effective vegetation management program. FAC-008 is a documentation-based standard for Facility Ratings Methodology whose execution is accounted for in FAC-009. While both are heavily violated Reliability Standards historically, a review of FAC-009 can lead to the determination of compliance with FAC-008. Additionally, FAC-009 requires coordination of facility ratings, which opens those ratings to peer review as a further check. In that case the Requirements of FAC-008 are not considered Tier 1 Requirements.

IRO – Interconnection Reliability Operations and Coordination

IRO-002-2, IRO-004-2, IRO-005-3a, and IRO-006-5 have been identified as high priority Reliability Standards. IRO-002 determines the sufficiency of tools needed for the RC to perform its role in maintaining the reliability of the BPS, which becomes increasingly imperative when emergency situations arise and Balancing Authorities and Transmission Operators require oversight. IRO-004 covers the planning the Reliability Coordinators must perform and ensures preparations are properly made for seen and unseen emergency events in the operation horizon. IRO-005 contains the only Tier 1 Requirement applicable to the PSE function. It is expected that the Regional Entities will ensure all PSEs are audited according to a six year interval cycle, including those PSEs which were removed from the 2011 audit schedule. For audits of PSEs, Regional Entities will provide a complete audit report regardless of audit scope. IRO-006 discusses the process of transmission load relief (TLR), and while this is an important topic, performance is

covered in IRO-005, and therefore the Requirements of IRO-006 are not considered Tier 1 Requirements.

MOD – Modeling, Data, and Analysis

MOD-001-1a, MOD-004-1, and MOD-008-1 have been identified as high priority Reliability Standards. These three Reliability Standards determine the procedure by which Available Transmission Capability (ATC) is to be calculated by Transmission Service Providers. The proper setting of ATC is vital so facilities are not overloaded, which could lead to possible system emergencies. FERC has mandated that this standard be audited following regulatory approval of the Reliability Standard.

NUC – Nuclear

NUC-001-2 has been identified as a high priority Reliability Standard. The Nuclear Plant Interface Requirements (NIPRs) in NPIR agreements are essential components of NUC-001-2. NERC strongly recommends that generation and transmission entities carefully review their respective obligations under these agreements, including coordinated communication to ensure that parties share a clear and precise understanding of their obligations under these agreements.

PER – Personnel Performance, Training, and Qualifications

PER-001-0.1 and PER-002-0 have been identified as high priority Reliability Standards. PER-001 grants operating personnel the authority to operate the system reliably, but this standard is addressed in many other Reliability Standards with more specific language based upon the function considered, and therefore the Requirements of PER-001 are not considered Tier 1 Requirements. PER-002 encompasses the development of training as well as the training itself of all operating personnel responsible for ensuring reliability of the BPS. Training, especially in preparedness for dealing with or the prevention of emergency events is essential.

PRC – Protection and Control

PRC-001-1, PRC-004-1, PRC-005-1, PRC-007-0, PRC-008-0, PRC-011-0, and PRC-023-1 have been identified as high priority Reliability Standards. PRC-001 promotes understanding of the limitations and performance of protection systems, which is especially important from an operational standpoint such that protection systems are not overloaded and the system cannot be controlled. PRC-004 is a particularly important standard as it applies to misoperations analysis and reporting. As significant protection system misoperations are considered disturbance events, those misoperations for which BPS reliability is affected that are always addressed in PRC-004 are captured by EOP-004 R3 as well, and therefore the Requirements of PRC-004 are not considered Tier 1 Requirements. . Significant misoperations are those that result in such actions as modifications to operating procedures or equipment and identification of lessons learned as identified by Attachment 1 to EOP-004.

PRC-005 is the most violated standard of all time, and its mission to organize and implement protection system maintenance is especially critical for ensuring system reliability. PRC-007 and PRC-008 deal with underfrequency load-shedding (UFLS) while PRC-011-0 involves undervoltage load-shedding (UVLS). Both UFLS and UVLS protection systems are important, but the level of compliance of a Registered Entity with PRC-005 will be most telling for compliance with these Reliability Standards. As a result, the Requirements of PRC-007, PRC-008, and PRC-011 are not considered Tier 1 Requirements. PRC-023, as with all Reliability Standards, has the chief purpose of promoting reliability in the BPS, and in this case it relates to transmission relay protection settings. The concerns surrounding these settings are that they are proper for detecting and protecting against fault conditions. As with UFLS and UVLS maintenance programs, the compliance performance of a registered entity with PRC-005 is a good guide as to how well protection systems at that entity are maintained and tested, which is applicable to PRC-023 as an indicator of the due diligence of an entity in properly setting relays and reviewing transmission system protection schemes. Also, significant misoperations resulting from improper relay settings are addressed through EOP-004, which would allow for a complete review of Requirements in PRC-023 in response to any such event. For those reasons listed, the Requirements of PRC-023 are not considered Tier 1 Requirements.

TOP – Transmission Operations

TOP-001-1, TOP-002-2a, TOP-003-0, TOP-004-2, TOP-006-1, and TOP-008-1 have been identified as high priority Reliability Standards. TOP-001 sets down operation authority for the TOP function, and in so doing, re-iterates language from the EOPs and IROs addressing this same issue. In an event where it can be demonstrated that an operator was not aware of his authority to act, this standard will be important for an entity to be audited on. However, as the authority of system operators is generally well understood, and therefore the Requirements of TOP-001 are not considered Tier 1 Requirements.. TOP-002 deals with normal operations planning, and one of the key concepts to this standard is communications. The outage coordination that is discussed in TOP-003 is implied by TOP-002 in normal operations planning, and therefore the Requirements of TOP-003 are not considered Tier 1 Requirements. . TOP-004 addresses operating in an unknown state and points to insufficient or faulty equipment, processes, planning, etc. and should be considered a high priority issue especially in terms of preparedness for emergencies. TOP-006, the monitoring of reliability parameters, can be gauged from compliance with TOP-008, which complements IRO-005 but this time for the TOP function. The Requirements of TOP-006 will not be considered Tier 1 Requirements while TOP-008 will be.

TPL – Transmission Planning

TPL-003-0a and TPL-004-0 have been identified as high priority Reliability Standards. TPL -003 accounts for the loss of two or more BPS elements, and TPL-004 addresses extreme events, both of which go hand-in-hand with minimizing the impact of emergency events affecting the system. By accounting for N-2 system losses in TPL-003 and losses of several elements in TPL-004, even if projects are not constructed to mitigate all issues

that are identified, acknowledgement of and familiarity with potential events will allow for expedited recovery, should one actually occur.

CMEP Discovery Methods

Compliance Audits

The Reliability Standards selected for compliance audit are determined based on the 2012 Implementation Plan Methodology. The Regional Entities will provide to the registered entity the scope of the compliance audit with the audit notification letter. The scope document will contain the Regional Entities' analysis of their risk and performance-based approach, which determines the audit scope for the registered entity being audited. The intervals for compliance audits is three years for entities registered as a Reliability Coordinator, Balancing Authority, or Transmission Operator, and is six years for entities registered for all other functions³¹. Registered Entities may be audited more frequently as needed based upon the results of risk and performance based assessments performed by the Regional Entities as well as the facts and circumstances surrounding.

Regional Entities have the authority to expand an audit to include other Reliability Standards and Requirements, but cannot reduce the scope without NERC's consent. Regional Entities shall consider past performance, including historical violation trends across the Region and those specific to the registered entity, and changes to compliance responsibility resulting from mergers, acquisitions, corporate re-organizations, open investigations and other factors that in the judgment of the Regional Entity audit staff should be considered as part of the normal planning required for a compliance audit and consistent with generally accepted audit practices.

Regional Entity audit teams are authorized and obligated to expand the scope of a compliance audit to include Tier 2 and Tier 3 Requirements and any other requirements they may deem necessary based on the results of the Registered Entity Profile Assessment or the audit team's collective professional judgment. Audit scope expansion can occur at any point during the process, from the initial review of the Registered Entity Profile Assessment through the close of the audit.

The scope of the registered entities' compliance audits will include a review of all mitigation plans³² that are open during the on-site audit, as discussed in the CMEP. Regional Entities must provide the compliance audit team with the status, documentation and evidence for all mitigation plans that are to be reviewed.

Should an expanded scope be required based upon significant issues discovered during the on-site portion of the audit process, the audit team will have the discretion to schedule

³¹ See Rules of Procedure, Section 403.11.1 at http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20110412.pdf

³² See Appendix 4C of the NERC RoP at Sections 3.1.4.3 and 6.6: http://www.nerc.com/files/Appendix4C_Uniform_CMEP_20110101.pdf

a follow-up spot check for reviewing the registered entity's compliance with the Reliability Standards and Requirements forming the expanded scope. The audit team will issue a new 30-day notification letter for a spot check in order to allow the registered entity proper time to prepare evidence necessary for the expanded audit scope. The additional compliance monitoring performed by the audit team as a result of the expanded audit scope should not exceed the current audit period.

For compliance audits, NERC provides additional guidance:

Audit Focus or Scope

To increase the efficiency of compliance audits in 2012 the Regional Entity audit teams will have the option of limiting the review of processes and procedures to the Registered Entity's current, in-force documentation, and to the implementation of the Registered Entity's internal compliance program. The audit teams will have the flexibility to review historical information on an as needed basis; this approach allows the audit team to focus on the current reliability risk and determining compliance. In accordance with NERC's RoP³³, documentation submitted to audit teams must be signed, either directly or electronically, by an authorized representative of the registered, regardless of whether or not the document is current or historical. In the event a finding of a possible violation is determined based upon the current, in-force documents, the audit team will review previous versions of the process and procedure documentation to determine the full extent of the possible violation.

In 2012, the audit period, being the range of time for which a registered entity is audited, will be individual to each entity based upon several factors. Depending upon a registered entity's particular situation, the start date for the audit period may be one of several possibilities:

1. the day after the prior audit, or
2. when other monitoring activity by the Compliance Enforcement Authority ended, or
3. the later of June 18, 2007 or the Registered Entity's date of registration if the Registered Entity has not previously been subject to a Compliance Audit.

The end date for the period of time to be covered during compliance audits in 2012 will be the end date for the compliance audits as outlined in the current CMEP, Section 3.1.4.2³⁴.

It should be noted that, except for those entities that have been recently registered, all Balancing Authorities (BAs), Transmission Operators (TOPs), and Reliability Coordinators (RCs) have experienced at least one compliance audit prior to the end of

³³ See Section 3.0 of Appendix 4C of the NERC RoP at:
http://www.nerc.com/files/Appendix4C_Uniform_CMEP_20110101.pdf

³⁴ See Appendix 4C of the NERC RoP at
http://www.nerc.com/files/Appendix4C_Uniform_CMEP_20110101.pdf

2010. For these Registered Entities that have undergone compliance audits already, all available versions of supporting documentation were reviewed for the entire audit periods, which began on June 18, 2007 and ended at their respective audit completion dates.

CIP Reliability Standards Compliance Audits

Registered entities are subject to audits for compliance with all Requirements of CIP-002-3 through CIP-009-3, which took effect October 1, 2010. If there are indications of possible non-compliance, auditors are authorized and obligated to review an entity's compliance throughout the entire audit period, which includes previous versions of CIP Reliability Standards, in order to determine the extent of possible violations.

If a responsible entity has active Technical Feasibility Exceptions (TFEs), Section 8 of NERC RoP - Appendix 4D³⁵, Procedure for Requesting and Receiving TFEs to NERC CIP Standards requires that subsequent Compliance Audits of the Responsible Entity conducted prior to the Expiration Date shall include audit of implementation and maintenance of the compensating measures and/or mitigating measures and implementation of steps and conduct of research and analyses towards achieving Strict Compliance with the Applicable Requirement. These topics are to be included in Compliance Audits regardless of whether the audit was otherwise scheduled to include the CIP Standard that includes the Applicable Requirement. Audit Team Leads of CIP audits will have requisite experience, training, and/or credentials in cyber security and/or IT auditing due to the need for subject matter expertise and the complexity of these Reliability Standards.

2012 Compliance Audit Schedule

The 2012 ERO compliance audit schedule, which is a compilation of all regional schedules, will be posted on the Compliance Resource page on the NERC website.³⁶ This posted schedule is updated at least quarterly, allowing the Registered Entities to have access to the schedule for the upcoming year as soon as possible.

The compliance audits listed on the schedule are labeled as on-site audits or off-site audits. This distinction is only relevant to the location of the audit activities, not the rigor of the audits. Both on-site and off-site audits are compliance audits and are performed using the same Reliability Standards Audit Worksheets (RSAW) and other audit tools and processes. The major difference is that on-site audits would entail physical access to the audited entity's premises. In fact, a large portion of the pre-audit work associated with an on-site audit may actually occur off-site.

Nevertheless, certain types of audits must contain an on-site component because of the nature or functions of the Registered Entity. For example, Reliability Coordinator, Balancing Authority and Transmission Operator functions must be audited on-site. For other BPS users, owners, and operators on the NERC Compliance Registry, the Regions and NERC can use discretion on the location and the conduct of the audit. In either case, the Regional Entity should plan the audit to assure proper scope and rigor.

³⁵ http://www.nerc.com/files/Appendix4D_TFE_Procedures_20110412.pdf

³⁶ <http://www.nerc.com/commondocs.php?cd=3>

As a final note regarding the audits of entities registered for the PSE function, it is expected that the Regional Entities will ensure all PSEs are audited according to a six year interval cycle, including those PSEs which were removed from the 2011 audit schedule.

Compliance Audit Reports

Regional Entities are obligated to provide written audit reports for all compliance audits and spot checks in accordance with *NERC Compliance Process Directive #2010-CAG-001 - Regional Entity Compliance Audit Report Processing*³⁷. NERC posts all public versions of the Regional Entities' compliance audit reports of registered entities on the NERC website to satisfy requirements of the CMEP. Regional Entities submit two audit reports for each compliance audit of a Registered Entity: a public report and a non-public report. The public report does not contain critical energy infrastructure information or any other information deemed confidential. The public report does not include a description of how the audit team determined its findings; rather, it includes a listing of the findings. The names of the Regional Entity personnel and registered entity personnel participating in the audit are excluded from the public report, and all participants are identified by title. In accordance with FERC expectations³⁸, the non-public report shall document all areas of concern related to situations that do not appear to involve a current or ongoing violation of a Reliability Standard requirement, but instead represent an area of concern that could become a violation. The non-public report contains confidential information and detailed evidence that supports the audit findings. The names and titles of all Regional Entity personnel and all registered entity personnel participating in the audit are included in the non-public report.

Public and non-public compliance audit reports that do not contain possible violations are completed by the Regional Entities and are submitted to NERC at the same time. Upon receipt of the reports NERC posts the public reports on its website and submits the non-public audit reports to the applicable regulatory authority.

Public and non-public audit reports that contain possible violations are submitted to NERC at different times. The non-public compliance audit reports are completed by the Regional Entities as soon as practical after the last day of the audit and are then submitted to NERC. Upon receipt of the non-public reports, NERC submits them to the Applicable Governmental Authority. The public reports that contain possible violations are completed by redacting all confidential information in the non-public reports. The Regional Entities retain the public version of compliance audit reports that contains possible violations until all violations are processed through the NERC CMEP. Due process is considered complete when all possible violations are dismissed or when a violation is confirmed or a settlement is reached and a decision has been rendered, if applicable, by the regulatory authority (e.g. Notice of Penalty (NOP) has been issued in

³⁷ <http://www.nerc.com/page.php?cid=3|22>

³⁸ *Compliance with Mandatory Reliability Standards*, "Guidance Order on Compliance Audits Conducted by the Electric Reliability Organization and Regional Entities," 126 FERC ¶ 61,038 (2009) at P13, <http://www.nerc.com/files/GuidanceOrderOnComplianceAudits-01152009.pdf>

the United States). Upon completion of due process, the Regional Entities submit the public version of the compliance audit reports to the registered entities for review and comment prior to submitting them to NERC. Upon receipt of the public reports NERC posts them on the NERC website³⁹.

In order to promote transparency and to provide the industry with guidance for improving compliance, NERC will be publishing a document containing the areas of concern, lessons learned, recommendations, and suggestions developed by ERO audit teams as part of the compliance monitoring process for 2011. This document will be similar to the Case Notes⁴⁰ that NERC currently provides in regard to the lessons learned as a result of registered entities completing their mitigation plans. The document will not mention or make reference to any registered entities specifically, but will instead focus on those various aspects for supporting and helping to enhance compliance programs.

Compliance Tools

The RSAWs are designed to add clarity and consistency to the assessment of compliance with Reliability Standards. The RSAWs are used for multiple compliance monitoring methods. Comments on these and any of the ERO's auditor resources are welcome and can be directed to the Regional Entity Compliance Managers⁴¹.

The RSAWs are posted on the NERC public website⁴² 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 Regional Entities 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 Regional Entities and registered entities check the NERC website regularly to ensure the latest available versions of RSAWs are being used.

NERC works with Regional Entities to review these RSAWs on a continual basis for improvement. NERC plans to migrate RSAWs to a database format in the future to support timely updates as Reliability Standards are approved, modified, or retired.

Mitigation Plans

Registered Entities must be in compliance with all Reliability Standards at all times. NERC and the Regional Entities encourage aggressive self-assessments and analysis and self reporting of noncompliance by registered entities. Registered entities are further encouraged to draft mitigation plans upon identification and self reporting of possible violations, prior to the required submission timeline per the CMEP. Mitigation plans are not an admission of a violation and are treated as voluntary corrective action. However, mitigation plans duly prepared and promptly submitted to the Regional Entity will be

³⁹ Public audit reports can be found at: <http://www.nerc.com/page.php?cid=3|26|246>

⁴⁰ <http://www.nerc.com/page.php?cid=3|22|371>

⁴¹ Information concerning Regional Entity programs is available at: <http://www.nerc.com/page.php?cid=3|23>

⁴² <http://www.nerc.com/page.php?cid=3|22>

used to demonstrate a positive, proactive culture of compliance in any potential enforcement action.

Self-Certification

All registered entities are required to participate in the annual self-certification each year per the NERC Actively Monitored Reliability Standard list. Regional Entities, at their discretion, may include additional Reliability Standards to include in the Regional 2012 Implementation Plan. Registered entities will receive guidance and instruction from their respective Regional Entity concerning self-certification submittals. Self-certification is an important component of the ERO Compliance Monitoring and Enforcement Program. It is one of the discovery methods that monitor a Registered Entity's compliance with Reliability Standards, especially those that have not been included in audit scopes in recent years. Self-certification waivers are not available as all applicable Reliability Standards must be self-certified.

CIP-002-3 through CIP-009-3 Reliability Standards

Registered entities are required to self-certify once per year, as scheduled by the Regional Entity and according to the Regional Entity's 2012 Implementation Plan. However, self-certification may expand to include CIP supplemental questionnaires as directed by NERC or an Applicable Governmental Authority. For further information, refer to Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities⁴³.

A unique characteristic of the CIP Standards pertains to self-certification: CIP-002-3 R4 requires all entities to annually approve their risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets, even if such lists are null. Thus, entities will need to submit self-certification for CIP-002-3 even if they conclude they have no Critical Assets.

The requirements for Self-Certification differ from the reporting requirements for approved TFEs. TFE reporting requirements for Responsible Entities are described in Section 6 of NERC RoP - Appendix 4D, Procedure for Requesting and Receiving TFEs to NERC CIP Standards.

Spot Checks

Spot checks are compliance audits with a much narrower focus, but are performed with the same rigor as a compliance audit. NERC and the Regional Entities have the authority to conduct spot checks of any regulatory approved Reliability Standards. Regional Entities may expand the list of Reliability Standards and Requirements they have scheduled for spot checks in their Regional Implementation Plan. Regional Entities shall ensure, however, that they satisfy all spot check requirements in the NERC Reliability

⁴³ http://www.nerc.com/docs/standards/sar/Imp-Plan_Newly_Identified_CCA_RE_clean_last_approval_2009Nov19.pdf.

Standards, RoP, and CMEP. Regional Entities are obligated to provide written audit reports for all compliance audits and spot checks in accordance with *NERC Compliance Process Directive #2010-CAG-001 - Regional Entity Compliance Audit Report Processing*⁴⁴. The standard audit report template and procedure provided in NERC Compliance Process Directive #2010-CAG-001 will be used for all spot check reports.

CIP Reliability Standards

Selected Reliability Standards Requirements of CIP-002-3 through CIP-009-3 will be audited and additional spot checks may be performed at the Regional Entity's discretion. CIP audits, including CIP spot checks, will require the appropriate reports per the RoP, CMEP, and *NERC Compliance Process Directive #2010-CAG-001 - Regional Entity Compliance Audit Report Processing*⁴⁵.

Periodic Data Submittals

Specific Reliability Standards and Requirements have been identified for periodic data submittals. The periodic data submittals for 2012 are as shown on the Requirements Tab of the 2012 Actively Monitored Reliability Standards list. Specific information regarding periodic data submittals is defined in the Regional Entity Implementation Plans.

Self-Reporting

Registered Entities are encouraged to self-report compliance violations with any regulatory authority-approved Reliability Standard. In most cases, self-reports of compliance violations are provided to the appropriate Regional Entity.⁴⁶ The ERO strongly encourages Registered Entities to report violations of Reliability Standards as soon as possible to ensure that the entity receives any potential cooperation credits⁴⁷ for self-reporting⁴⁸ and minimizing any ongoing risk to the BPS.

Exception-Reporting

Specific Reliability Standards and Requirements in the 2012 Actively Monitored Reliability Standards list have been identified for exception reporting. The Registered Entities are expected to report to the Regional Entities for all events or conditions occurring that are exceptions to the associated Reliability Standard Requirement.

Reporting Credit

⁴⁴ <http://www.nerc.com/page.php?cid=3|22>

⁴⁵ <http://www.nerc.com/page.php?cid=3|22>

⁴⁶ The exception would be where the self-reporting entity is itself a Regional Entity, in which case the self-report should go directly to NERC in accordance with the Regional Entity's delegation agreement and other agreements with NERC.

⁴⁷ *North American Electric Reliability Corporation*, "Order on Review of Notice of Penalty," 134 FERC ¶ 61,209 (2011) at P 13, <http://www.ferc.gov/whats-new/comm-meet/2011/031711/E-3.pdf>

⁴⁸ *Guidance o Filing Reliability Notices of Penalty, North American Electric Reliability Corporation*, "Order on Review of Notice of Penalty," 124 FERC ¶ 61,015 (2008) at P 32, <http://www.ferc.gov/EventCalendar/Files/20080703131349-AD08-10-000.pdf>

Currently, self-reporting credits will not be given to those registered entities for filing reports they are required to make⁴⁹. Additionally, there are no reporting credits available during the enforcement process for mandatory reporting of self-certifications and self-reports during or after an audit. Cooperation credits may be available to a registered entity during the enforcement process based on facts and circumstances.

NERC has requested a rehearing on the issue of self-reporting credits from FERC⁵⁰. NERC recognizes that self-reporting credit is a critical component to entity compliance and BPS reliability and encourages registered entities to continue to self-report all possible violations as soon as possible.

Complaint

All regulatory authority-approved Reliability Standards or Requirements can be the subject of a complaint regarding a compliance violation by a Registered Entity. Complaints, if validated, can initiate one of the other compliance monitoring methods in order to determine the full extent of potential non-compliance.

NERC maintains a Compliance Hotline that is administered by the Event Analysis & Investigation (EA&I) group. Any person may submit a complaint to report a possible violation of a Reliability Standard by calling 404-446-2575, sending an e-mail directly to hotline@nerc.net or completing the form on <https://www.nerc.net/hotline/>. Unless specifically authorized by the complainant, NERC and Regional Entity staff will withhold the name of the complainant in any communications with the violating entity. All information provided will be held as confidential in accordance with the NERC Rules of Procedure. EA&I will informally seek additional information regarding the potential violation of Reliability Standards from the submitter and others, as appropriate. EA&I may refer the matter for further investigation by NERC or the appropriate Regional Entity.

Note: The NERC Compliance Hotline is for reporting complaints or possible compliance violations of Reliability Standards by an entity. For other questions regarding the NERC CMEP or Reliability Standards, please send an email to compliancefeedback@nerc.net.

Compliance Investigations

A Compliance Investigation may be initiated at any time by the NERC or the Regions in response to a system disturbance, Complaint, or the possible violation of a Reliability Standard identified by any other means. Compliance Investigations are confidential, unless FERC directs otherwise and are generally led by the Regional Entity's staff. NERC reserves the right to assume the leadership of a Compliance Investigation.

The Compliance Enforcement Authority reviews information to determine compliance with the Reliability Standards. The Compliance Enforcement Authority may request additional data and/or information as necessary through formal Requests for Information, site visits, sworn statements, etc. to perform its assessment.

⁴⁹ *North American Electric Reliability Corporation*, "Order on Review of Notice of Penalty," 134 FERC ¶ 61,209 (2011) at P 47, <http://www.ferc.gov/whats-new/comm-meet/2011/031711/E-3.pdf>

⁵⁰ http://www.nerc.com/files/FinalFiled_Req_For_Clarification_Turlock_Order_20100418.pdf

ERO Compliance Monitoring and Enforcement Program Organization

The focus of the ERO Enterprise's compliance program is to improve the reliability of the BPS in North America by fairly and consistently enforcing compliance with regulatory approved Reliability Standards. Specifically, the program is designed to ensure that the right practices are in place so that the likelihood and severity of future system disturbances are substantially reduced, while recognizing that no Reliability Standards or enforcement process can fully prevent all such disturbances from occurring. In order to fulfill these responsibilities the NERC compliance organization is comprised of four primary groups: Compliance Operations, Compliance Enforcement, Event Analysis and Investigation, and Regional Entities.

- The overriding goal of the Compliance Operations Department is ensuring success of the Regional Entities and registered entities with respect to reliability compliance.
- The Compliance Enforcement Department is tasked with ensuring strong, consistent, and expeditious enforcement of Reliability Standard violations.
- The Event Analysis and Investigation Department combines the technical expertise of NERC's situation awareness staff, events analysis staff and its event investigators to facilitate efficient processing of these complementary activities to provide lessons learned, which will promote increased reliability of the BPS.
- The Regional Entities execute the CMEP on behalf of the ERO according to their respective Regional Delegation Agreements.

In addition to the ERO's responsibilities, the CMEP (RoP Appendix 4C) states that all entities that are registered in the NERC Compliance Registry have the obligation to comply with all enforceable Reliability Standards for the functions for which the entity is registered. All registered entities are subject to the compliance monitoring methods included in the CMEP, and should be aware of their obligations. Every registered entity should have an aggressive internal compliance program for identifying and performing its CMEP responsibilities. Also, the registered entities are encouraged to participate in the Reliability Standards development process, recognizing that the Reliability Standards serve as the basis for compliance.

Compliance Enforcement

Program Scope and Functional Description

NERC's Compliance Enforcement department conducts all of NERC's enforcement activities, including:

- Docketing of all possible violations coming into the NERC enforcement program,
- Prosecution of compliance violation matters arising out of NERC-led investigations and audits,
- Review of all mitigation plans and dismissals approved by Regional Entities,
- Processing of all compliance violations prosecuted by Regional Entities, and
- Analysis of compliance statistics.

2012 Goals and Deliverables

A priority for this department is to achieve greater efficiencies in enforcement processing by focusing both NERC and Regional Entity compliance enforcement resources on the cases that have the most significant impact on the reliability of the BPS. This should reduce the overall ERO compliance caseload by ensuring that the number of cases processed through the filing of a notice of penalty exceeds the number of cases coming into the ERO docket and should thus allow NERC to close out cases expeditiously to provide timely lessons learned to the industry. NERC's Compliance Enforcement staff has realized significant efficiencies and expects to gain efficiencies through better utilization of existing resources in the future.⁵¹

Despite efforts to attain greater efficiencies, a significant gap is anticipated in the number of cases coming into the enforcement process and the number of cases the enforcement team can close out on a monthly basis. In the past year, as reflected in Figure 3, the ERO's caseload of active violations expanded from 2006 in January 2010 to 3193 in

⁵¹ There is substantial evidence of this increased efficiency. In 2010, Compliance Enforcement rolled out new risk-based processes in early 2010. These processes, including the introduction of the Disposition Document, Abbreviated Notice of Penalties, and other process improvements, have helped streamline compliance enforcement. Over the course of the year, Compliance Enforcement has also increased collaboration with Regional Entities and increased the number and expertise of Enforcement Staff. As a consequence, Compliance Enforcement has increased by 3.5 times the number of violations processed each month in 2010 compared to the number of violations processed each month in 2009 (70/month vs. 20/month).

An administrative citation process was initiated in January 2011 that will enable NERC and the Regional Entities to address new violations by submitting a single streamlined NOP covering numerous lower risk violations. See North American Electric Reliability Corporation, 134 "Notice of No Further Review of Initial Administrative Citation Notice of Penalty," 134 FERC ¶ 61,157 (2011) ("March 3, 2011 Order").

As of September 30, 2011, the compliance enforcement initiative will introduce a new enforcement process that will retire the administrative citation process. This is described in further detail below, in the 'Key CMEP Activities and Initiatives' section of the implementation plan.

January 2011. The rate of new violations coming into the case load has increased dramatically from an average of 140 violations per month in early 2010 to an average of 203 violations per month at the start of 2011. 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. As reflected in Figure 4, the number of incoming violations each month from non-CIP Reliability Standards has been relatively stable since June 2008, but with the staged implementation of the CIP Reliability Standards, the number of incoming violations each month from CIP Reliability Standards continues to rise.

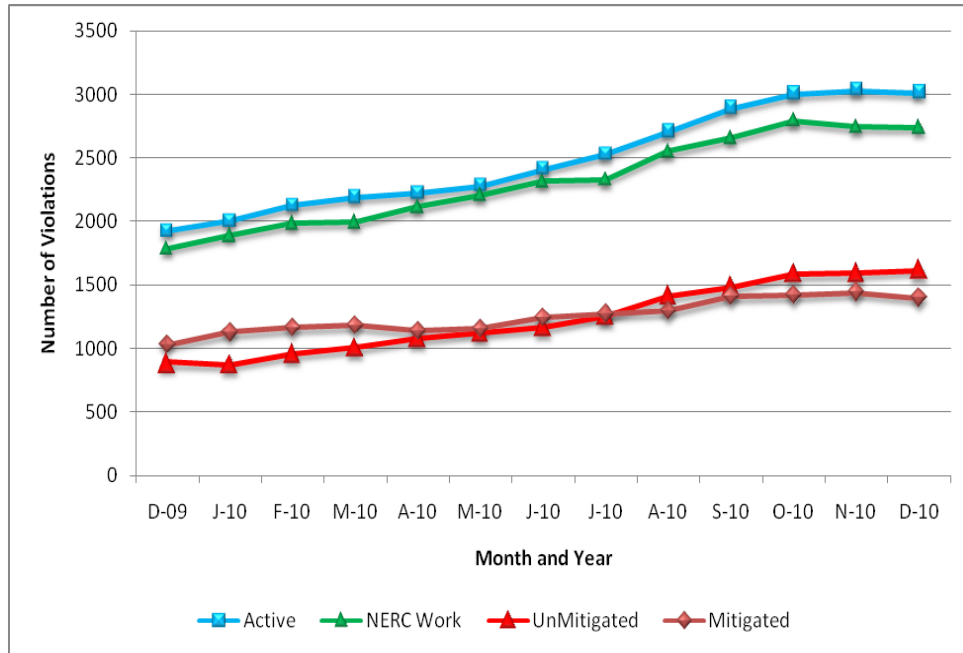


Figure 3: Compliance Processing Statistics for Calendar Year 2010.

The influx of new violations is expected to outstrip the number of violations NERC can process each month. Compliance Enforcement processed to BOTCC approval an average of 70 violations per month in 2010. With the implementation of streamlined procedures and the advent of the administrative citation process, the team has processed an average of 130 violations per month for the first three months of 2011. Still, further streamlining is required to reduce the overall caseload. NERC staff is actively working with Regional Entities and registered entities to develop further ways in which to streamline the enforcement process and ensure that enforcement resources are efficiently deployed to address the most significant risks to bulk power system reliability.

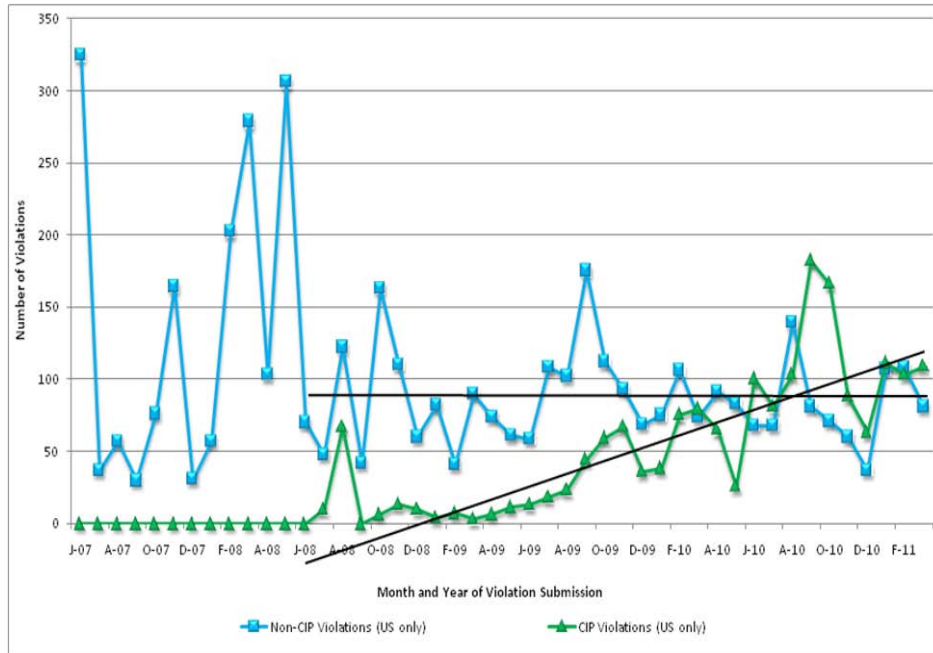


Figure 4: Violations Submitted per Month (CIP vs. Non-CIP).

Beyond management of the caseload, another significant area of focus for the next year will be to improve the submittal and completion of mitigation plans. As reflected in Figure 1 above, the increase in active violations in 2010 brought with it an increase in the number of unmitigated violations and a decline in the overall percentage of active violations subject to a mitigation plan. Currently, less than half of the active violations in the caseload have been mitigated, and a number of violations dating back to 2007 are not yet covered by mitigation plans. To help manage risk to the BPS, Compliance Enforcement will focus on understanding and improving upon the mitigation process.

Key CMEP Activities and Initiatives

NERC and the Regional Entities receive CMEP implementation feedback from the Members Representative Committee (MRC), Compliance and Certification Committee (CCC) and other stakeholders through the use of audited entity feedback forms. All feedback and input from these groups, among others, are reviewed on a continual basis for opportunities for improvement. NERC and the Regional Entities are committed to continuous improvement of the CMEP implementation.

CMEP Transparency Elements

NERC and the Regional Entities continuously balance the request from the industry to improve transparency with the confidential nature of the CMEP processes. Figure 5 is a pictorial view of the compliance process, and it shows how most of the processes in the CMEP fall under a window of confidentiality. NERC and the Regional Entities are continuously identifying and implementing innovative ways to share CMEP process information while honoring confidentiality. Additional initiatives are underway to increase transparency of CMEP elements in 2011. They are discussed later in this Chapter.

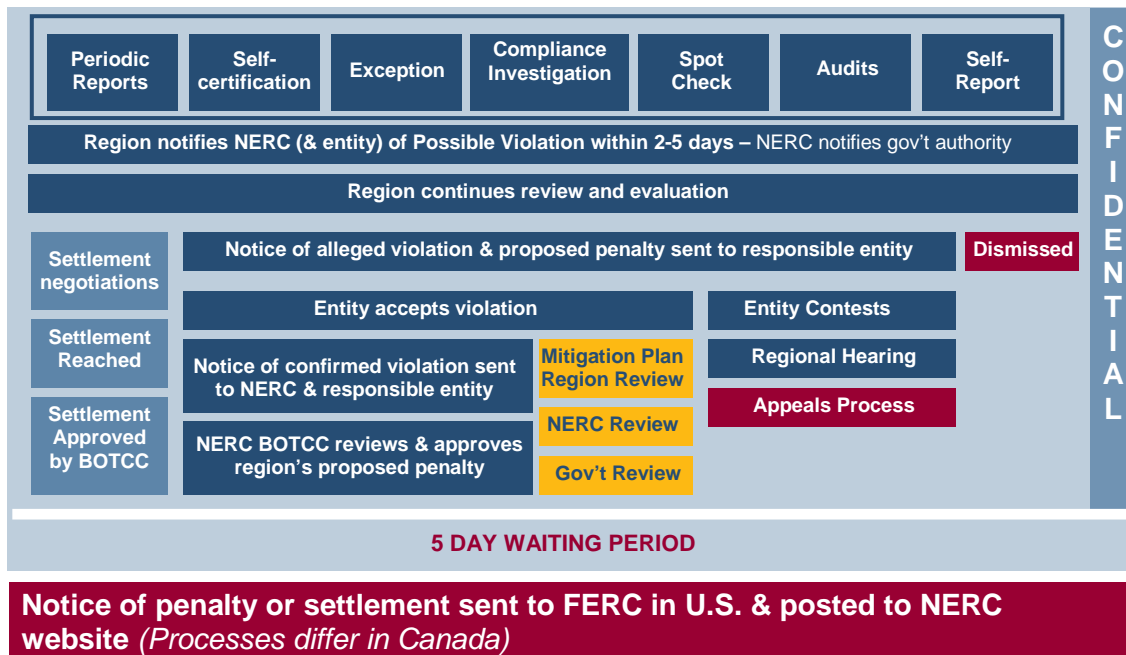


Figure 5: Compliance Process

In 2010, NERC began publicly posting CMEP implementation and process information. NERC Compliance Operations will continue to review and publicly post CMEP implementation and process information in the form of public notices⁵² in order to increase transparency of the CMEP application to registered entities.

⁵² Public notices are available at: <http://www.nerc.com/page.php?cid=3|22>

Compliance Operations and REs Communications

Seminars and Workshops

Seminars and workshops for compliance activities are conducted at both the Regional Entity and NERC levels. Each Regional Entity provides Compliance Workshops at least once a year. NERC offers four workshops per year for registered entities. Two of these workshops focus on “Standards and Compliance,” and two of these workshops focus on assisting registered entities in improving their compliance programs. The seminars and workshops are important learning exercises for those subject to Reliability Standards. NERC and the Regional Entities will continue compliance seminars, workshops and panel discussions to educate registered entities and to increase transparency of CMEP processes that are important to reliability.

Transparency Communications

The NERC Compliance Operations Program and the Regional Entities are working toward common goals related to improving consistency, increasing transparency, and creating more efficiency in compliance processes. Past field experience gained by Regional Entities and NERC is an important part of meeting the goal to provide clarity on particular items and state the proper expectations. NERC provides transparency information in various formats, depending on the scope of the matter and relevance to the particular functions within the BPS. These include the following, as well as other means as NERC deems necessary:

CANs – Compliance Application Notices⁵³

CANs focus on current and future auditable compliance applications. CANs provide continued compliance and enforcement guidance as a means to facilitate information to industry while Reliability Standards are revised and improved as discussed in FERC Order No. 693.

CARs – Compliance Analysis Reports⁵⁴

CARS are a historical look at compliance trends for individual Reliability Standards and will include addendums when the information is updated.

Case Notes⁵⁵

Case Notes provide examples of mitigation plans for recent possible violations that have not completed processing through an enforcement action. Case notes do not identify the Registered Entity.

Bulletins⁵⁶

Bulletins provide general information or clarification on current and future issues.

⁵³ <http://www.nerc.com/page.php?cid=3|22|354>

⁵⁴ <http://www.nerc.com/page.php?cid=3|329>

⁵⁵ <http://www.nerc.com/page.php?cid=3|22|371>

⁵⁶ <http://www.nerc.com/page.php?cid=3|22>

Directives⁵⁷

Directives provide notice of a mandatory action and guidance for Regional Entities.

Lessons Learned⁵⁸

Lessons Learned result from an event analysis. They provide examples of how a problem occurred and was identified, and the corrective action taken.

Annual CMEP Reports⁵⁹

Annual CMEP Reports are assessment of the previous year's CMEP and are used in the planning and development of future years' annual CMEP Implementation Plans.

Compliance Application Notices

CANs provide necessary compliance guidance and fulfill NERC's obligations under FERC Order No. 693 to provide compliance guidance going forward.

In FERC Order No. 693⁶⁰ several commenter's argued there were gaps and ambiguities in the standards and requested relief from monetary penalties and even compliance with the Reliability Standards. According to paragraph 274 FERC opined, "As discussed in our standard-by-standard review, each Reliability Standard that we approve contains Requirements that are sufficiently clear as to be enforceable and do not create due process concerns."

Further, in Order No. 693 paragraph 277, the Commission agreed with NERC that, even if some clarification of a particular Reliability Standard would be desirable at the outset, making it mandatory allows the ERO and the Regional Entities to provide that clarification on a going-forward basis while still requiring compliance with Reliability Standards.⁶¹

Thus, the Compliance Application Notice (CAN) serves two purposes:

1. To provide *transparency to industry* on how an ERO compliance enforcement authority will apply compliance criteria to determine possible non-compliance with a NERC Reliability Standard; and
2. To *establish consistency in the application of compliance criteria* across all compliance enforcement authorities.

In practice, auditors must make in-the-field determinations of what constitutes possible non-compliance of a Reliability Standard. In essence, the auditor, without guidance,

⁵⁷ <http://www.nerc.com/page.php?cid=3|22>

⁵⁸ <http://www.nerc.com/page.php?cid=5|385>

⁵⁹ <http://www.nerc.com/page.php?cid=3|26>

⁶⁰ FERC Order No. 693, Docket No. RM06-16-000 (March 16, 2007).

⁶¹ "NERC can maximize consistency and appropriateness of treatment in compliance matters most efficiently if it has the ability to advise or provide direction...at an early stage...." FERC Order on NERC Three Year Assessment, Docket Nos. RR09-7-000 and AD10-14-000, §216.

must make an interpretation of the standard. A CAN attempts to gather the practices that occur in the field, and, if the practices are consistent, provide transparency of the compliance application to industry. In the event that auditor practices vary, the posted CAN establishes a consistent compliance application that all auditors will adopt going forward. The implementation of this type of compliance application may create some change as it drives consistency across the ERO.

A CAN provides significant advantages to industry. Registered Entities will have visibility into how compliance will be applied and will be able to depend upon the compliance application being consistent across auditors and regions. In the event that an inconsistency occurs, a registered entity will be able to point to the CAN as the auditable compliance application. Additionally, CANs can be generated in a relatively short period – approximately three months – compared to the codified Standards Development Process,⁶² which may take longer than a year.

CANs are posted for a three-week industry comment period. All comments that are received for each CAN are carefully reviewed and considered. Industry comments are especially important when the compliance application varies across auditors or regions, as the CAN will establish a consistent application.

NERC's belief is that transparent, open communication is beneficial, and transparency of compliance applications provides an opportunity to formally address areas of concern. When industry disagrees with the compliance application identified in a CAN, there are existing processes that continue to be available for formal resolution. A registered entity may:

1. request a formal interpretation;⁶³ or
2. submit a Standard Authorization Request (SAR) to modify the standard; or
3. if a registered entity is found to have a non-compliance based on the compliance application identified in a CAN, to contest the violation; or
4. submit a technical rationale why the compliance application is incorrect or should be modified.

The compliance application identified in a CAN will be retired when a future standard or interpretation that addresses the issue – either by supporting the CAN or changing it – has been approved by FERC and is enforceable. Further, a CAN may be revoked or revised if additional information is brought forward to demonstrate that the CAN is incorrect.

As of June 29, 2011, there are 16 CANs posted as final on the NERC website and 26 additional CANs in various stages of the development process, plus over 20 CAN requests pending development.

⁶² See the NERC Rules of Procedure, Appendix 3A, Standards Process Manual, Effective September 3, 2010.

⁶³ An interpretation is conducted through the Standards Development Process. As such, it is formally filed with FERC and will result in an order issued by FERC Commissioners.

Compliance Analysis Reports

Registered entities can use Compliance Analysis Reports (CAR) and any corresponding addendums to view historical information on highly violated Reliability Standards and those most critical to reliability. For those Requirements in each standard that have similar violation descriptions for multiple registered entities, NERC and the Regional Entities provide suggestions for registered entities to improve their programs to comply with the Requirements. The registered entities can also see the discovery method of each of the violations. If the registered entities have a high percentage of violations discovered through self-reports or self-certifications, it shows an aggressive ICP. If the standard has a high percentage of violations discovered through compliance audits, there should be some concern that the registered entities are uncertain how to comply. The report serves as a mechanism to deliver some clarity and information to improve compliance.

Regional Entities can use the reports to point out any regional issues that may have resulted from the violations that could involve compliance, registration, or enforcement issues. They can also use the violation descriptions to improve consistency on auditing to the standard.

Training

Compliance Auditors

The NERC compliance auditor training is based in part on generally accepted auditing practices found in documents such as the Government Accounting Office (GAO) Generally Accepted Government Auditing Standards, and is revised from time to time. Continuing education will provide training on specific auditing issues to promote consistency and increased reliability.

In 2012, NERC Compliance Operations will design and develop a tiered system of qualifications for compliance staff with requisite testing and/or credentials. Training is an important part of delivering consistency across NERC and the Regions.

In addition, NERC sponsors seminars on specific matters as a way to provide continuous education to ERO staff. Two such seminars were performed in 2011, and two are scheduled for 2012.

Specialized training for CIP auditors was performed in 2011 and will continue in 2012. It is intended not only to address technical issues unique to the CIP Standards environment, but also to increase the skills of CIP auditor staff. Two sessions of CIP Standards Training (CIP Basics for Auditors) are scheduled for 2012. NERC encourages the CIP audit staff to have requisite experience, training and credentials in cyber security and IT auditing.

Compliance Investigative (CI) Staff

A “Fundamentals of CI” course/seminar has been conducted for NERC and Regional Entity staff by NERC over the last two years. The training is scheduled to be conducted twice annually and is revised from time to time.

Mitigation Plans

Non-Confirmed Violations Without Submitted Mitigation Plans

In 2010, Compliance Enforcement staff began analyzing various violation processing trends for the Board of Trustees Compliance Committee and for stakeholders. A trend has been identified in an increasing number of active violations in NERC's violation processing database for which the registered entities have not yet submitted mitigation plans. While there are a number of different reasons for the increase, NERC would like to remind registered entities of the importance of timely mitigation plans and that the submission of a mitigation plan is not an admission of a confirmed violation. Voluntary correction of possible violations in a timely manner may also reduce the potential of a penalty consistent with section 4.3.3 of NERC's Sanctions Guidelines⁶⁴.

Compliance Enforcement staff will continue to clarify that the submission of a mitigation plan is not an admission of confirmed violation. Prior to, and if, enforcement confirms a possible violation to an alleged violation, the mitigation plan is treated as a voluntary corrective action. The evidence collected by ERO enforcement will determine whether a violation exists.

Registration and Certification

The purpose of the Organization Registration Program is to clearly identify those entities that are responsible for compliance with the regulatory approved Reliability Standards and is described in the NERC Rules of Procedure Appendix 5A Organization Registration and Certification Manual. As described in the NERC Statement of Compliance Registry Criteria, NERC will include in its compliance registry each entity that the ERO concludes can materially impact the reliability of the BPS. NERC is obligated to identify all organizations to be listed in the NERC compliance registry. Identifying these organizations is necessary and prudent 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.

Multi-Regional Registered Entities (MRRE)

There are several activities related to registration, compliance monitoring and enforcement involving registered entities that are registered and operate and/or conduct business in multiple regions. NERC and the Regional Entities have worked together to develop a process for MRREs that will delineate the CMEP implementation for these types of registrations. The purpose of the Multi-Regional Registered Entity (MRRE) process is to describe the coordinated CMEP processes that will be used by NERC and the Regional Entities for a subset of registered entities that are registered in multiple regions on a voluntary basis. The MRRE process allows these entities the ability to request to be accountable to one Compliance Enforcement Authority (CEA). This

⁶⁴ See Appendix 4B *Sanction Guidelines of the North American Electric Reliability Corporation* from NERC's Rules of Procedure at: http://www.nerc.com/files/Appendix4B_Sanction_Guidelines_20110101.pdf

coordinated process provides for increased efficiencies in compliance resource allocation for NERC, the Regional Entities, and the registered entities while maintaining the reliability of the BPS. Due to potential Regional Entity jurisdictional issues, the MRRE process is on hold as of May 2011 pending NERC legal's review and determination of these issues.

Joint Registration Organization and Coordinated Functional Registration

Joint Registration Organization (JRO)⁶⁵: In addition to registering as the entity responsible for all functions that it performs itself, an entity may register as a JRO on behalf of one or more of its members or related entities for one or more functions for which such members or related entities would otherwise be required to register, and, thereby, accept on behalf of such members or related entities all compliance responsibility for that function or those functions, including all reporting requirements.

Coordinated Functional Registration (CFR)⁶⁶: In addition to registering as an entity responsible for all functions that it performs itself, multiple entities may each register using a CFR for one or more reliability standard and/or for one or more requirements/sub-requirements within particular reliability standards applicable to a specific function. The CFR submission must include a written agreement that governs itself and clearly specifies the entities' respective compliance responsibilities. The registration of the CFR is the complete registration for each entity. Additionally, each entity shall take full compliance responsibility for those Reliability Standards and/or requirements/sub-requirements it has registered for in the CFR. Due to abrupt or forced registration changes, as described below, this form of registration may become more common in 2012.

Results of Abrupt or Forced Registration Changes

The conclusions drawn from a of the EOP-005 System restoration and Blackstart Compliance Analysis Report completed by NERC indicate that an increasing number of self-reported Possible Violations (PVs) are being issued due to abrupt or forced registrations.

As such, these types of PVs involve a heavier case load for Registered Entities, as some of the violations require lengthy mitigation plans. Furthermore, for issues that involve certifiable functions, a NERC certification must be completed per the Rules of Procedure.

NERC and the Regional Entities will continue to work together in the development of appropriate actions to efficiently manage the compliance issues resulting from abrupt and forced registration changes.

⁶⁵ Section 507 of the NERC RoP,
http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20110412.pdf

⁶⁶ Section 508 of the NERC RoP,
http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20110412.pdf

The Compliance Enforcement Initiative

After five years as the ERO, NERC continues to seek ways to improve and adapt its processes and Reliability Standards. NERC, 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 Compliance Enforcement Initiative (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 resolving issues that do not pose a serious risk to the reliability of the BPS, more resources can be focused on violations that do pose a risk to reliability.

The CEI is being launched in accordance with NERC’s existing rules and procedures. The new initiative is not about whether issues will be addressed. Rather, it is about how they are addressed.

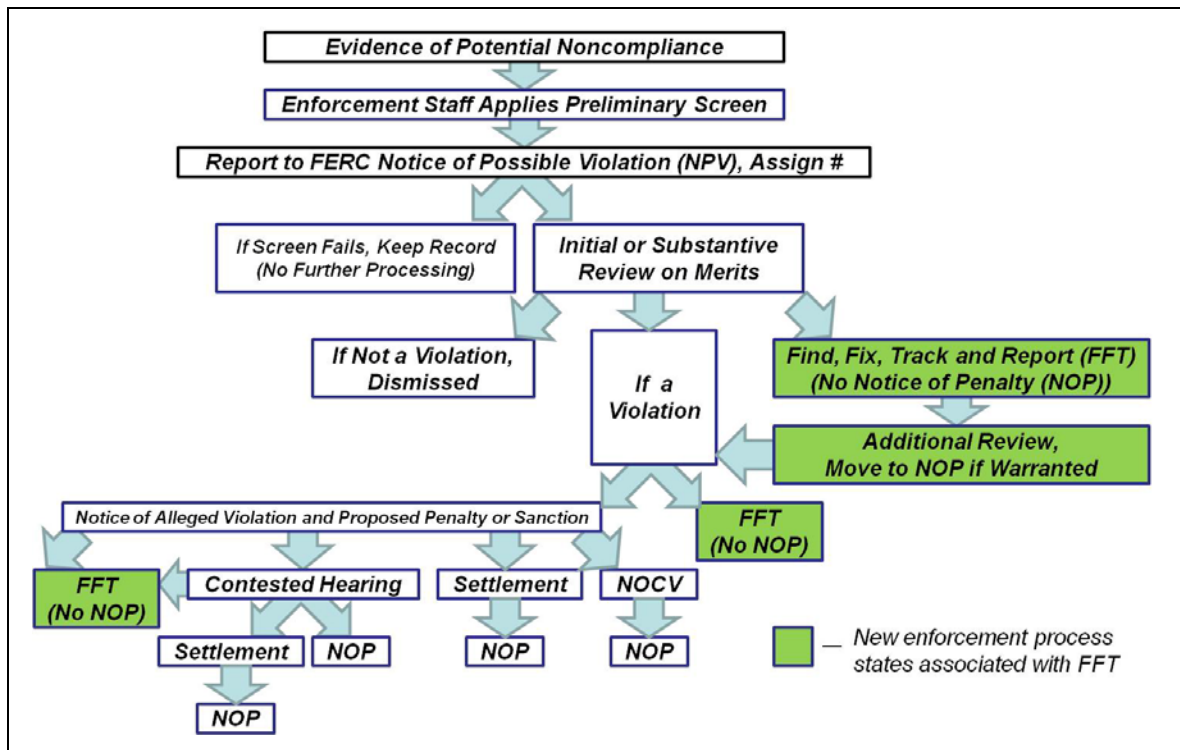


Figure 6: New Enforcement Process incorporating the Find, Fix, Track, and Report (FFT) Approach.

Following NERC's filing⁶⁷ of the CEI on September 30, 2011, there will be three possible tracks, see Figure 6, for dealing with compliance matters: Dismissal; Find, Fix, Track and Report (FFT); and Notice of Penalty (NOP). Dismissals occur where there are no violations, when the entity is not registered for and/or 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 Possible Violation poses a lesser (minimal to moderate) risk to bulk power system reliability. All matters identified via FFT or NOP must be fixed; the registered entity must provide a statement of completion and completion of mitigation activities is subject to verification by the Regional Entity as part of an audit, spot check or random sampling. The issue must be fixed prior to inclusion in a report to FERC. A Possible Violation processed through the FFT track becomes a remediated issue once included in an FFT informational filing and such filing concludes processing of that matter by Regional Entities 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 bulk power system, NOPs will be filed. They may be filed either in a spreadsheet format or a full NOP format.

Regions 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 Phase I, which is targeted to occur over a 12-18 month period after the initial kickoff of the CEI at the end of September 2011. During Phase I, compliance staff may make recommendations to enforcement staff for ultimate disposition of an issue as part of an FFT or NOP. In Phase II, both compliance and enforcement staff may determine the ultimate disposition of an issue.

Almost 70 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 Possible Violation is awaiting a determination of which processing track it will be treated with. This will help illustrate that the registered entity understands the full scope of the violation and has taken actions to correct it and prevent recurrence.

⁶⁷ 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

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 lesser 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 Possible Violations 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 bulk power system, NERC is able to better fulfill its mission as the ERO.

Events Analysis Interface with Compliance

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/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/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 who make a good faith effort to self-identify and self-disclose possible violations stemming from their event analyses will be afforded consideration in any enforcement action in accordance with NERC's Sanction Guidelines. If further analysis by the Regional Entity or NERC reveals other possible violations, 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.

To facilitate the development of a rigorous self-assessment, NERC Events Analysis has developed the Compliance Analysis Template, which is found in Appendix G of its process.⁶⁸ Additionally, this Compliance Analysis Template is attached below as Appendix 5.

⁶⁸ See page 35, Appendix G, "Electric Reliability Organization Event Analysis Process": http://www.nerc.com/files/2011-05-02%20Event_Analysis_Process_Phase%20%20Field%20Test%20Draft%20-%20Final%20-%20For%20posting.pdf

Regional Entities CMEP Implementation Plans

The Regional Entities Implementation Plan is an annual plan, submitted to NERC no later than October 1 of each year for approval that, in accordance with NERC RoP Section 401.6 and the NERC CMEP Implementation Plan, identifies:

1. All Reliability Standards identified by NERC in the 2012 CMEP Actively Monitored Reliability Standards list.
2. Other Reliability Standards proposed for monitoring by the Regional Entity; these will include any regional Reliability Standards and additional NERC Reliability Standards.
3. The methods to be used by the Regional Entity for reporting, monitoring, evaluation, and assessment of performance criteria with each Reliability Standard. NERC expects at a minimum for the Regional Entities to perform the compliance monitoring methods identified in the NERC 2012 Actively Monitored Reliability Standards list. When a Regional Entity determines that an increased audit scope is necessary, then the Regional Entity shall notify the registered entity of the increased audit scope. This notification shall be part of the audit notification package and shall include the Reliability Standards and Requirements that are included in the increased scope, as well as the justification for the increased scope. When a Regional Entity determines that an increased audit scope is necessary after the notification package is sent, or while the audit team is on-site, then the Regional Entity shall notify the registered entity of the increased audit scope as soon as possible. For references to NERC guidance or Implementation Plans such as the CIP Guidance, a link should be included in the Regional Entity Implementation Plan instead of listing the entire document.
4. The Regional Entity's Annual Implementation Plan should include a list of registered entity names that are on the 2012 schedule, NERC Compliance Registration ID, and the year they will be audited. The Regional Entity can provide its audit plan for multiple years in the future.
5. The Regional Entity's Annual Plan should address Key CMEP Activities and Initiatives.

Conclusion

The ERO CMEP Implementation Plan, which is developed according to Section 215(c) of the Federal Power Act, is the operating plan for annual compliance monitoring and enforcement activities. NERC, as the international ERO, and the Regional Entities through their delegation agreements with NERC, monitor and enforce compliance of registered entities with all regulatory approved Reliability Standards. Registered entities include all BPS owners, operators and users.

While the actions of the ERO in accordance with the CMEP are critical to the reliability of the BPS, it is only one part of an overall plan to ensure system reliability. The other part consists of the actions of the registered entities and the electric power industry at large, and these are equally as critical to system reliability. The registered entities must participate in the educational, informational and developmental efforts that are being undertaken not only to maintain reliability, but to enhance it as well. The sharing of the industry's technical expertise, experience, and judgment as well as its participation in the ERO's processes will help to further identify and remove reliability gaps and shortcomings. The ERO continuously seeks to improve the execution of its role in ensuring system reliability, as is the case with the advancements of the annual CMEP Implementation Plan undertaken for 2012, but the industry must continue to participate for the overall reliability plan to be successful.

Revision History

REVISION NUMBER	DATE	NATURE OF CHANGE	REVIEWER	APPROVAL
0	5/5/2011	Original Development	Jacki Power Craig Struck Kyle Howells Jodi Ernst	Michael Moon
0.1	6/3/11	Incorporated appropriate comments from NERC staff.	Jacki Power Craig Struck Kyle Howells	Michael Moon
0.2	6/25/11	Incorporated appropriate comments from FERC, Compliance and Certification Committee, and Regional Entities.	Jacki Power Craig Struck Kyle Howells	Michael Moon
0.3	6/30/11	Final review for content and formatting. Changed from Draft document to working document.	Jacki Power Craig Struck Kyle Howells Caroline Clouse	Michael Moon
0.4	7/5/11	Added references to Regional Entity input into AML and Implementation Plan on pages 6, 11, 12, and 16.	Craig Struck	Michael Moon
0.5	7/12/11	Incorporated appropriate comments from the NERC Board of Trustees Compliance Committee.	Craig Struck Kyle Howells Jodi Ernst	Michael Moon
0.6	8/1/11	Original posting. Editorial corrections made to Figure 5, Compliance Processes, on page 36.	Craig Struck	Michael Moon
0.7	8/25/11	Revised posting. Updates to Table 6 and Appendix 2 to reflect minor revisions to the 2012 AML as well as minor editorial corrections to the Implementation Plan	Kyle Howells	Michael Moon
1.0	10/19/11	Revised posting. Incorporated a description of the Compliance Enforcement Initiative as well as the Events Analysis Interface with Compliance. Updated the basis for NUC-001 inclusion into the 2012 AML.	Kyle Howells	Michael Moon
1.1	10/26/11	Updated Events Analysis Interface with Compliance language	Kyle Howells	Michael Moon
1.2	12/14/11	Incorporated guidance concerning the audits of entities registered as a PSE on pages 18 and 25.	Craig Struck	Michael Moon

Appendix 1 – 2012 ERO High-Risk Priorities with High Value Associated Reliability Standards

The ERO high-risk priorities are those current issues challenging the BPS. These issues have been identified through the analysis of significant events on the BPS, such as the August 2003 blackout, and the execution of compliance actions in addition to input provided by numerous groups, including the Regional Entities, NERC’s CEO, and many other industry stakeholders. Additionally, recent events within North America have highlighted several areas of importance within the BPS, and the lessons learned and circumstances surrounding these events have been taken into account as well. Therefore, the high-risk priorities are as follows:

1. **Misoperations of relay protection and control systems** – Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. Protection systems are designed to operate reliably when needed under the presence of a fault on the system, to quickly isolate a piece of equipment or a ‘zone’ of the BPS, without allowing the fault to transfer into adjoining facilities. The greater the number of facilities involved in an event, the more severe the impact to the rest of the BPS, with cascading failure such as the “Zone 3 Relay” issue in the August 2003 blackout being the extreme. Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization. Adding to the risk is that system protection is an extremely complex engineering field – there are many practitioners but few masters.
2. **Human errors by field personnel** – Field personnel play an important role in the maintenance and operation of the BPS. They often switch equipment in and out of service and align alternative configurations. Risks can be introduced when field personnel operate equipment in a manner that reduces the redundancy of the BPS, sometimes even creating single points of failure that would not exist normally. Taking outages of equipment to conduct maintenance is a routine and necessary part of reliable BPS operation. However, any alterations to the configuration of the network must be carefully planned in advance to minimize loss of redundancy and avoid unintended single points of failure. It is also important that such changes and risks be communicated to system operators and reliability coordinators in advance, so that they can make adjustments in their operating plans and reliability assessments.

3. **Ambiguous or incomplete voice communications** – Out of longstanding tradition, system operators and reliability coordinators are comfortable with informal communications with field and power plant personnel and neighboring systems. Experience from analyzing various events indicates there is often a sense of awkwardness when personnel transition from conversational discussion to issuing reliability instructions. It is also human nature to be uncomfortable in applying formal communication procedures after personnel have developed informal styles over many years. Confusion in making the transition from normal conversation to formal communications can introduce misunderstandings and possibly even incorrect actions or assumptions. Further, once the need to transition to more formal structure is recognized, the transition is often not complete or effective. Results can include unclear instructions, confusion as to whether an instruction is a suggestion or a directive, whether specific action is required or a set of alternative actions are permissible, and confusion over what elements of the system are being addressed.
4. **Right-of-way maintenance** – The August 14, 2003 blackout highlighted effective vegetation management programs as a key recommendation for avoiding future cascading failures. More broadly, any encroachments in the right-of-way that reduce clearances to the point of lowering facility ratings or reducing the randomness of possible contacts can be a risk to reliability. Although these impacts may not always be readily apparent, under extreme wind and temperature conditions they may become more of a risk to BPS reliability. There are many challenges to effective right-of-way maintenance, especially maintaining proper clearances, including interventions by private landowners, local municipalities, and federal and state landowners.
5. **Changing resource mix** – Energy and environmental policies along with energy markets are driving proposals toward unprecedented changes in the resource mix of the BPS. Examples include integration of significant amounts of renewable energy (variable such as wind and solar), natural gas, storage and demand resources to provide energy and capacity. Industry’s knowledge of the characteristics of the BPS comes from nearly a century of operational experience with the existing resource mix. However, integration of these new resources results in operating characteristics significantly different from conventional steam production facilities. An array of reliability services must be provided over a range of time horizons from seconds to minutes to hours and days, and annually such as load following, contingency reserves, frequency response, reactive supply, capacity and voltage control, and power system stability. Continued reliable operation of the BPS will require an industry dialog with policymakers and regulators. Understanding the impacts on reliability will depend on accurate modeling of new resources, and development of new methods and tools for the provision of essential reliability services.

6. **Integration of new technologies** – While the electric utility industry was once thought to be slow in adopting new technologies, smart grid initiatives across the country have proven this not be the case as of late. To continue this proactive trend of incorporating new technologies as well as to ensure proper coordination, a number of Reliability Standards should be considered in order to make this priority possible. Introduction of electric vehicles, demand-side management, variable generation, distributed resources and smart grid technologies presents tremendous opportunities but also introduces changes to the operating characteristics of the BPS. Integration of these new technologies requires changes in the way the BPS is planned and operated to maintain reliability. Further, additional tools/models are required to support their integration to meet policy and strategic goals. Without these changes, it will be challenging to maintain reliability with large-scale deployments. For example, some smart grid devices/systems increase exposure to cyber threats, while variable generation requires additional ancillary services. Integration of these new technologies must be achieved in a manner that does not undermine existing levels of stability, resilience and security of the BPS.
7. **Preparedness for -impact, low-frequency events** – Although there is a wide range of threats labeled “high-impact, low-frequency,” the greatest concern is being prepared for possible events that could debilitate the BPS for extended periods, such as widespread, coordinated physical/cyber attacks or geomagnetic storms. The industry must consider improving the design of the BPS to address these potential risks, prepare coordinated North American response plans for use during catastrophic events, and be ready to deploy those plans to restore essential services in a timely manner.
8. **Non-traditional threats via cyber-security vulnerabilities** – Establishment of enterprise risk-based programs, policies and processes to prepare for, react to, and recover from cyber-security vulnerabilities is a high priority for the industry. The BPS has not yet experienced wide-spread cyber-attacks, and a contributing factor has been the traditional physical separation between the industrial control system/SCADA environment and the business and administrative networks. This situation, however, is rapidly changing, predominantly due to the efficiencies that can be achieved by leveraging shared networks and resources, so now even physically separated environments are susceptible. For example, the BPS could be as vulnerable to digital threats as IT systems, but with far more critical implications, as the recent Stuxnet virus has shown. Disabling or turning systems off in a binary fashion is concerning enough, but as illustrated by Stuxnet, industrial control system software can be changed and data can be stolen without intrusions even being detected. These injection vectors serve as a blueprint for future attackers who wish to access controllers, safety systems, and protection devices to insert malicious code-targeting changes to set points and switches as well as alteration or suppression of measurements.

9. Other

Certain considerations that have potentially high impacts to reliability do not fit cleanly into other categories. Such considerations include the Frequency Response Initiative and Winter Weather Events from the Southwest and Texas in February of 2011. The Reliability Standards relating to these considerations, especially those corresponding to emergency procedures, are important in terms of enacting lessons learned and preventing detrimental conditions in the future.

NERC has identified a number of Reliability Standards associated with each of the ERO high-risk priorities. These associated Reliability Standards have a high value in that they most directly address the concerns raised by the high-risk priorities. The relationships of these high-value Reliability Standards to the high-risk priorities are laid out in the list below.

1. Ambiguous, Incomplete Voice Communications

- COM-002
- EOP-002
- EOP-005
- EOP-006
- EOP-008
- IRO-002
- IRO-006
- TOP-002

2. Mis-Operations of Relay and Controls Systems

- EOP-005
- EOP-008
- FAC-001
- PRC-001
- PRC-004
- PRC-005
- PRC-023
- TPL-003
- TPL-004

3. Human Errors by Field Personnel

- COM-002
- EOP-005
- EOP-008
- FAC-003
- PER-002

4. High-Priority CIP and Supporting Standards

- CIP-001
- CIP-002
- CIP-005
- CIP-006
- CIP-007
- COM-001
- COM-002
- EOP-005
- EOP-008

5. Right-of-Way Maintenance and Clearances

- FAC-003
- FAC-008
- FAC-009
- TOP-002
- TPL-003
- TPL-004

6. Changing Resource Mix

- EOP-001
- EOP-005
- EOP-002
- IRO-002
- TOP-002

7. High-Impact, Low-Frequency Events

- EOP-003
- EOP-005
- EOP-008
- IRO-004
- IRO-005
- NUC-001
- TOP-004
- TOP-007

8. Other

- Frequency response initiative
 - BAL-003
- Winter Weather Events (Texas, February 2011)
 - BAL-002
 - EOP-001
 - EOP-002
 - EOP-004
 - EOP-005

9. Integration of New Technologies

- COM-001
- FAC-001
- FAC-002
- FAC-009
- IRO-002
- PRC-001

Appendix 2 – 2012 Actively Monitored List (AML) Analysis

As with the Reliability Standards selected for audit in 2012, the Reliability Standards selected for annual self-certification in 2012 represent the results of a risk-based approach. Due to the breadth of the AML, it can be helpful to perform targeted analysis in order to corroborate that the ERO priorities are being properly addressed. As a synopsis of the AML, Table 8 shows a breakdown of the applicable requirements within the AML for 2012 and in years past. The average number of Requirements per function for 2012 has been reduced substantially from previous years. In fact, since the CIPs have been incorporated into the AML in 2010, the average number of Requirements by function has been reduced to half of its maximum; there were an average of 167 Requirements to be audited per function in 2010 while there are 84 in 2012.

Table 8: Requirements Analysis for the 2012 AML and those going back to 2007

Function	Requirements Analysis								
	Total Applicable Reqs as of 1/1/2012	2012 AML (All Reqs)	2012 AML (CIP only)	2012 AML (693 only)	2011	2010	2009	2008	2007
TOP	499	170	109	61	246	321	134	142	115
RC	397	136	109	27	203	299	97	131	76
BA	408	155	109	46	206	305	107	175	95
TO	369	134	107	27	222	271	70	86	86
GO	302	119	107	12	198	242	34	47	40
GOP	254	121	109	12	168	242	27	38	13
TSP	318	166	107	59	202	206	5	7	2
RSG	20	2	0	2	0	6	6	20	20
PA/PC	178	6	0	6	42	88	56	89	86
TP	143	13	0	13	49	83	51	86	86
IA	184	107	107	0	145	168	0	0	0
RP	22	3	0	3	3	0	0	0	0
LSE	267	123	109	14	157	214	12	26	13
PSE	11	1	0	1	1	3	3	4	3
DP	129	9	0	9	51	54	21	51	51
Avg Reqs	233	84	65	19	126	167	42	60	46

When looking at the total number of in-effect Requirements as of January 1, 2012 within the 2012 AML as applicable by function, there is a strong correlation between the potential reliability impact of a function and the proportion of its applicable Requirements that are represented on the 2012 AML. For instance, the Reliability Coordinator, Balancing Authority, and Transmission Operator certified functions, all have over 30% of their applicable Requirements on the AML. For other functions, such as the Purchasing-Selling Entity (PSE) or Distribution Provider (DP), a much smaller proportion of their Reliability Standards is incorporated. These results are shown in Table 9.

In some cases, such as the TSP, Generator Operator (GOP), Interchange Authority (IA), and Load-Serving Entity (LSE), there is perhaps an unexpectedly high percentage of applicable Reliability Standards within the 2012 AML. The TSP has a large number due to the inclusion by FERC Order 729 of MOD-001, MOD-004, and MOD-008, which alone count for 76 Requirements. The GOP, IA, and LSE functions have a large proportion of Requirements due to

CIP. Looking at Table 10, which is similar to Table 9 but accounts only for 693 Reliability Standards, the GOP, IA, and LSE functions are shown to have 15%, 0%, and 15% of applicable 693 Requirements within the 2012 AML respectively, which are much more reasonable numbers.

Table 9: Percent of total in effect Requirements as of 1/1/2012 represented in the 2012 AML

Requirements Analysis			
Function	Total Applicable Reqs as of 1/1/2012	2012 (All Reqs)	% of Total
TOP	499	170	34%
RC	397	136	34%
BA	408	155	38%
TO	369	134	36%
GO	302	119	39%
GOP	254	121	48%
TSP	318	166	52%
RSG	20	2	10%
PA/PC	178	6	3%
TP	143	13	9%
IA	184	107	58%
RP	22	3	14%
LSE	267	123	46%
PSE	11	1	9%
DP	129	9	7%

Table 10: Percent of total in effect 693 Requirements as of 1/1/2012 represented in the 2012 AML

Requirements Analysis			
Function	Total Applicable 693 Reqs as of 1/1/2012	2012 (693 Reqs)	% of Total
TOP	327	61	19%
RC	225	27	12%
BA	236	46	19%
TO	201	27	13%
GO	134	12	9%
GOP	82	12	15%
TSP	150	59	39%
RSG	20	2	10%
PA/PC	178	6	3%
TP	143	13	9%
IA	16	0	0%
RP	22	3	14%
LSE	95	14	15%
PSE	11	1	9%
DP	129	9	7%

Table 11 shows that only 29.72% of all Requirements within the three tier structure are included in the 2012 AML, which is represented by Tier 1 Requirements.

Table 11: Requirement counts by Tier

2012 AML - Tier 1	Tier 2	Tier 3
274	397	251

The following figures, Figure 6 and 7, display the information discussed already, but provides it in a different format for ease of comparison. Figure 6 displays the number of AML Requirements by registered function across all years of mandatory compliance in addition to the total number of applicable Requirements as of January 1, 2012. Figure 7 shows the same information, but only for the 2012 AML and the total number of applicable Requirements as of January 1, 2012.

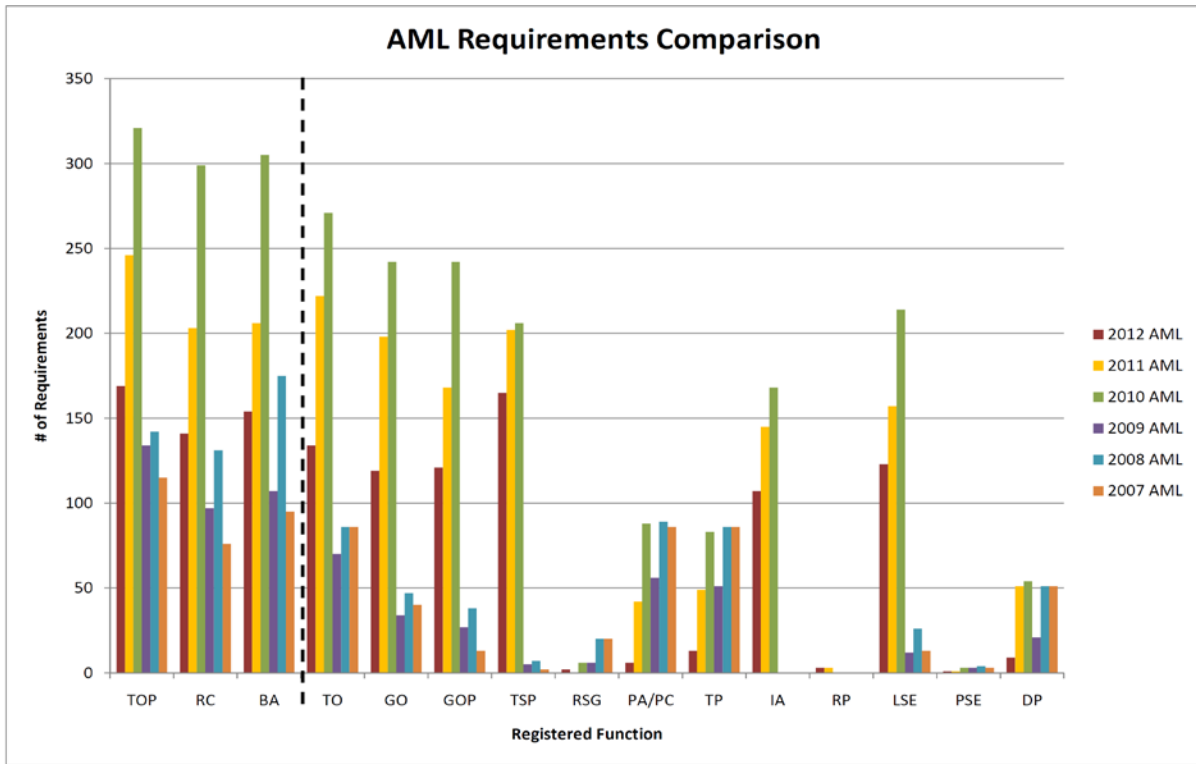


Figure 6: Number of applicable Requirements to each function within a given year's AML and for all Requirements currently in effect.

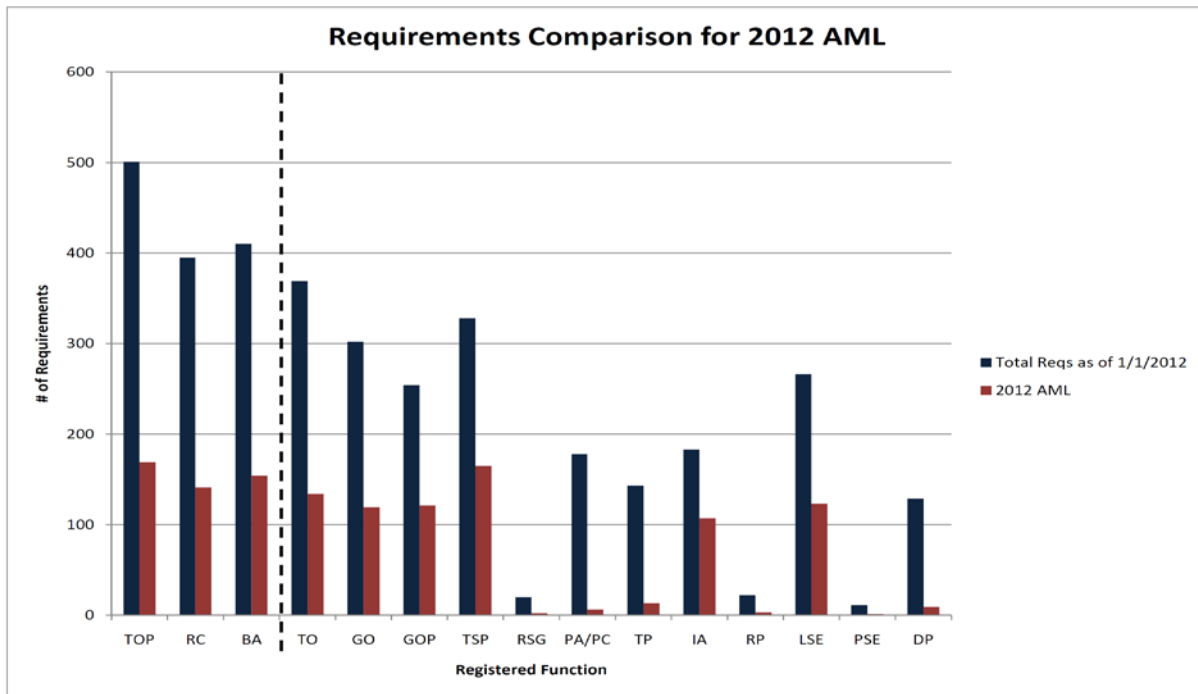


Figure 7: Direct comparison of Requirements in the 2012 AML as compared to all in effect Requirements as of 1/1/2012.

CONFIDENTIAL (NON-PUBLIC)

Appendix 3 – 2012 Regional Entity Request to Defer or Reduce the Scope of a Compliance Audit

Request to Reduce Scope or Deferment of a Compliance Audit

This form should be submitted as both a Word and PDF file to NERC Compliance Operations at least 90 days prior to the audit for approval. Email forms to Jacki.Power@nerc.net and Stacia-Ann.Chambers@nerc.net

Requesting Regional Entity Information

Date:	
Name:	
Title:	
Region:	
State the basis for Reduced Audit Scope or Deferment of Compliance Audit:	
State other methods used for compliance monitoring during period of reduced scope or deferment?	
State requested duration of deferment, if applicable.	
State whether this is a MRRE audit?	
Applicable Region(s):	FRCC <input type="checkbox"/> MRO <input type="checkbox"/> NPCC <input type="checkbox"/> RFC <input type="checkbox"/> SERC <input type="checkbox"/> SPP <input type="checkbox"/> TRE <input type="checkbox"/> WECC <input type="checkbox"/>

Registered Entity Information

Registered Entity's Legal Name:	
NCR ID Number:	
Date of Last Compliance Audit:	
Date of Next Compliance Audit:	

Regional Entity's Additional Information

Comments:	
-----------	--

Regional Entity Authorized Signature

ERO Analysis Results

State information reviewed and basis for determination	
--	--

ERO Final Determination

Approved: Declined:

ERO, Director of Compliance Operations

Appendix 4 – 2012 CMEP Implementation Plan Survey

Questions to the Regional Entities concerning the 2012 CMEP Implementation Plan

Instructions: Each Regional Entity shall complete the 2012 CMEP Implementation Plan Survey and provide it to NERC no later than January 31, 2013. This feedback is needed as soon as possible, as it will be used as input into the 2014 CMEP Implementation Plan and 2014 budget development.

I. Compliance Monitoring

1. Please provide statistics on the number and types of compliance audits conducted (Please separate CIP from Order 693 audits)
 - a. Were all planned audits completed?
 - i. If not, please indicate the reasons.
 - b. How many compliance audit reports were completed in 2012?
 - i. For the 693 compliance audit reports, did you complete them within the CMEP suggested timeframe of 60 days?
 - ii. If not, what challenges did you face for completing compliance audit reports?
2. Please provide statistics on the other methods used by the Regional Entity for reporting, monitoring, evaluation, and assessment of performance criteria with each Reliability Standard as indicated by your annual Implementation Plan (Please separate CIP from Order 693).
 - a. Were all mandatory Spot Checks completed?
3. Please provide a status of your three-year and six- year Compliance Audit program plan. Is your Regional Entity compliance audit program on schedule?
4. What actions did you take to address the Outstanding Issues list that NERC issues each month?
5. Do you have processes in place to monitor the progress of settlement negotiations to make sure they are progressing well?

II. Compliance Outreach

6. Please provide statistics on your Regional Compliance Workshop.
 - a. How many workshops?
 - b. Number of participants?
 - c. What feedback was received from the workshops?
 - d. What should be added to the workshops?
7. Describe any other communication mediums used to promote the consistency and transparency of the NERC Compliance Program for 2012?
 - a. How successful were your consistency and transparency efforts?

- b. What improvements are planned for 2013?

III. Compliance Enforcement

8. Please describe any efforts you have undertaken to improve the efficiency of your compliance enforcement process.
 - a. Utilization of NERC’s streamlined enforcement templates (disposition documents, settlement templates)
 - b. Participation in the administrative citation program
 - c. Staffing and other initiatives to improve efficiency
10. Please describe any efforts you have undertaken to improve mitigation of Reliability Standards violations.
 - a. Encouragement of prompt submission of mitigation plans
 - b. Monitoring of mitigation plan completion and encouragement of early mitigation plan completion
11. What has been your experience with the effectiveness of penalty and sanctions levied to incite compliance and eliminate repeat offenders?
12. What has been your experience in moving violations back into the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) process by ceasing negotiations and issuing a Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS)?

IV. Program Effectiveness

13. Describe any general observations, best practices, lessons learned, and trends for the Regional Entities as well as registered entities.
14. Describe any significant changes (e.g. process, communication changes) from the 2011 program that were implemented in your 2012 Regional Compliance Program.
 - a. What were the positive and/or negative experiences associated with these changes, if any?
15. Discuss any significant challenges encountered in 2012, describe the action taken, or suggest potential remedial actions.

V. Events Analysis and Compliance Reviews

16. How many events analyses were conducted in 2012 within your region?

VI. Projection for the Future

17. What changes would you propose to reduce the 2013 Actively Monitored List? How would you revise the risk-based criteria?
18. Do you have any specific recommendations for the NERC Compliance Monitoring and Enforcement Program that you would like to include in the NERC annual report this year?
19. How do you plan to address the “risk-based” approach in your auditing program?
20. What type of budget issues did you face in implementation of the 2012 CMEP? Are there any budgetary issues that need to be addressed for 2013

Appendix 5 – Events Analysis Process Appendix G - Compliance Assessment Template

Events Analysis Process Appendix G - Compliance Assessment Template

The registered entity’s compliance function is expected to perform an initial compliance assessment, concurrent with the registered entity’s event analysis process.

A systematic, methodical compliance assessment process might include the following steps:

1. Refer to the causes and contributing factors of the event as determined by the registered entity’s event analysis process.
2. Identify any applicable Reliability Standards requirement that may have been implicated by the causes and contributing factors of the event.
3. Develop conclusions after reviewing the facts and circumstances of the event that are relevant to step 2 above as they apply to the applicable Reliability Standards requirements.
4. Self-report any findings of non-compliance to the Regional Entity per the CMEP procedures.

Sample Template for Compliance Assessment Summary

Event causes or contributing factors	Applicable NERC Reliability Standards	Details of Compliance Assessment Effort	Findings
Cause	AAA-000-0 Requirement 1	Identify the process used to assess compliance with this requirement. Identify any evidence that demonstrates compliance. Identify any evidence that suggests non-compliance.	Findings of possible violations should be identified. If there are no findings of non-compliance, that should be noted.
	AAA-000-0 Requirement 2		
Contributing factor	BBB-000-0 Requirement 1		

Category 1a Example

Event causes or contributing factors	Applicable NERC Reliability Standards	Details of Compliance Assessment Effort	Findings*
Equipment failure of a high side transformer– cleared along with two transmission lines.	TOP-002-2a R6. Each BA and TOP shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, sub-regional and local reliability requirements.	Established transfer limits were followed such that the event did not result in instability. The limit for operating across this internal interface is established in the RC. “ <u>XYZ Interface All Lines In Stability Guide</u> ” (document provided)	No findings of non-compliance.*
Equipment failure of a high side transformer– cleared along with two transmission lines.	TOP-002-2a R10. Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	No SOLs were violated. There are no IROLs associated with the loss of equipment in this event. See the specific guide referenced in the response to TOP-002-2a R6 .	No findings of non-compliance.*
Equipment failure of a high side transformer– cleared along with two transmission lines.	TOP-004-2 R1. Each TOP shall operate within the IROLs and SOLs. R2. Each TOP shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.	The system was operated to remain within transfer limits across the “XYZ” internal interface established as a result of stability studies as delineated in the Transmission Operating Guide developed by RC. See the specific guide referenced in the response to TOP-002-2a R6 .	No findings of non-compliance*
Equipment failure of a high side transformer– cleared along with two transmission lines.	PRC-001 R1. Each TOP, BA and GOP shall be familiar with the purpose and limitations of protection system schemes applied in its area.	Both the RC and the TOPs are trained on the Transmission Operating Guides as well as relaying and SPSs on the BPS. Protection operated correctly and as planned.	No findings of non-compliance*
Equipment failure of a high side transformer– cleared along with two transmission lines.	PRC-004 R1. The TOP and any Distribution Provider that owns a transmission Protection System shall each analyze its transmission Protection System Misoperations and shall develop and implement a Corrective Action Plan to avoid future Misoperations of a similar nature according to the Regional Entity’s procedures.	System Protection engineers evaluated the relay operations and determined that all relaying operated correctly and as planned.	No findings of non-compliance*
Equipment failure of a high side transformer– cleared	TOP-008 R1. The TOP experiencing or contributing to an IROL or SOL	R1 Operators used their EMS-based tools to ensure that there were no	No findings of non-compliance*

<p>along with two transmission lines.</p>	<p>violation shall take immediate steps to relieve the condition, which may include shedding firm load. R2. Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the TOP shall always operate the BPS to the most limiting parameter. R3. The TOP shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the TOP shall notify its RC and all neighboring TOPs impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter. R4. The TOP shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The TOP shall use the results of these analyses to immediately mitigate the SOL violation.</p>	<p>SOL/IROL violations. R2 by following the TOP Guides developed by RC, violations do not occur. R3 no conditions occurred that required disconnection. R4 Operators used their EMS-based tools to ensure that there were no SOL/IROL violations.</p>	
<p>Equipment failure of a high side transformer– cleared along with two transmission lines.</p>	<p>TOP-006 R2. Each RC, TOP and BA shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources. R5 Each RC, TOP and BA shall use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.</p>	<p>The EMSs at both the RC and the TOP provide operators with the information needed to evaluate system conditions and notify operators when conditions are off normal. EMS system visibility and communications were not lost during this event.</p>	<p>No findings of non-compliance*</p>

			<p>*Findings as the outcome of a compliance self-assessment will result in either a statement of “No Findings” or that of “Possible Violation (PV).”</p> <p>Should the latter be the result, the entity will be given the opportunity to self-report the PV to the Regional Compliance Enforcement department, in accordance with the existing procedures set forth in the CMEP. In doing so, the entity self-reporting should inform the Regional Compliance Enforcement department that this has been done consistent with the event analysis process and the completion of a compliance self-assessment (Appendix G) to obtain the credit prescribed.</p>
--	--	--	---