

The logo for NERC, consisting of the letters "NERC" in a bold, black, sans-serif font. A horizontal blue bar is positioned below the letters.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

A tall, lattice-structured metal tower for a high-voltage power line, with several cross-arms extending horizontally. The tower is set against a light blue sky with a soft, hazy glow. The tower is positioned on the right side of the page, with a dark blue curved shape in the top right corner.

NERC Compliance Monitoring and Enforcement Program

2009 Implementation Plan

A faint, light blue map of North America is visible in the background of the lower half of the page. The map shows the outlines of the United States and Canada.

to ensure
the reliability of the
bulk power system

September 2008

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

Table of Contents

1. NERC Compliance Monitoring and Enforcement Program	1
2. Introduction	2
3. NERC Compliance Monitoring and Enforcement Program Organization	3
4. 2009 Program Implementation - Discovery	4
4.1 Application of Discovery Methods under the CMEP	4
4.1.1 <i>Compliance Audit and Self Certification</i>	4
4.1.2 <i>2009 Compliance Audit Schedule</i>	5
4.1.3 <i>Semi-Annual Self Certifications for CIP-002-1 through CIP-009-1 Reliability Standards</i>	5
4.1.4 <i>Spot Check</i>	6
4.1.5 <i>Periodic Data Submittals</i>	7
4.1.6 <i>Exception Reporting</i>	7
4.1.7 <i>Compliance Violation Investigation</i>	8
4.1.8 <i>Self Report</i>	8
4.1.9 <i>Complaint</i>	9
4.2 Reliability Standards Subject to 2009 CMEP Implementation.....	9
5. 2009 Program Implementation - Enforcement	14
5.1 Violation Reporting	14
5.2 Remedial Action Directives.....	15
5.3 Mitigation Plan Approvals.....	15
5.4 Regional Entity Validation of Completed Mitigation Plans	15
6. Improving Transparency and Consistency	17
6.1 Improve Transparency of the CMEP Implementation.....	17
6.1.1 <i>Yearly Compliance Audit Schedules</i>	18
6.1.2 <i>Status of Compliance Audit Reports</i>	18
6.1.3 <i>Reliability Standard Audit Worksheet</i>	19
6.2 Multiple Region Registered Entities (MRRE).....	20
6.3 Provide Feedback to the NERC Reliability Standards Development Process	20
6.4 Provide Information to the Industry about the CMEP	20
7. 2009 Regional CMEP Implementation Plans	20
Appendix A – Mitigation Plan Table	21

1. NERC Compliance Monitoring and Enforcement Program

Under Section 215(c) of the Federal Power Act¹ to establish and enforce Reliability Standards for the bulk power system, subject to review by the Federal Energy Regulatory Commission (FERC) (United States) and in general accordance with the “Principles for an Electric Reliability Organization that can Function on an International Basis,”² the North American Electric Reliability Corporation (NERC) Compliance Monitoring and Enforcement Program (CMEP) is designed to improve reliability through the effective and efficient enforcement of Reliability Standards.

To help fulfill its responsibilities under its rules filed with regulatory authorities, NERC, as an international electric reliability organization (ERO), formed under the Energy Policy Act of 2005,³ delegates authority to monitor and enforce compliance with Reliability Standards of users, owners and operators of the bulk power system to qualified Regional Entities that have executed a delegation agreement with NERC and approved by the appropriate regulatory authorities.

¹ http://www.nerc.com/fileUploads/File/AboutNERC/HR6_Electricity_Title.pdf

² Bilateral Electric Reliability Oversight Group, August 3, 2005 (the “Bilateral Principles”).

³ http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h6enr.txt.pdf#page=348

2. Introduction

The NERC CMEP Implementation Plan (Implementation Plan) is the strategic operating plan for annual compliance monitoring and enforcement activities to ensure NERC, as an international ERO, and its Regional Entities fulfill their responsibilities under the legislation in the United States and other applicable obligations in other jurisdictions in Canada and Mexico. The compliance monitoring and enforcement activities are carried out by NERC and the eight Regional Entities based on the regulatory-approved uniform Compliance Monitoring and Enforcement Program, the NERC Rules of Procedure, and their respective delegation agreements with the eight Regional Entities. This plan outlines the implementation requirements to be followed by NERC and the eight Regional Entities. Each Regional Entity shall submit its 2009 implementation plan by November 1, 2008 to NERC. NERC is responsible for approving the Regional Entity implementation plans.⁴

The 2009 Implementation Plan is based on:

- NERC Rules of Procedure
- Compliance Monitoring and Enforcement Program
- Regional Entity Delegation Agreements
- NERC Board of Trustees and regulatory-approved Reliability Standards
- History of the compliance activities and findings
- Input from reliability performance
- Risk based criteria scope for compliance audits and self certifications

The objectives of the Implementation Plan are to:

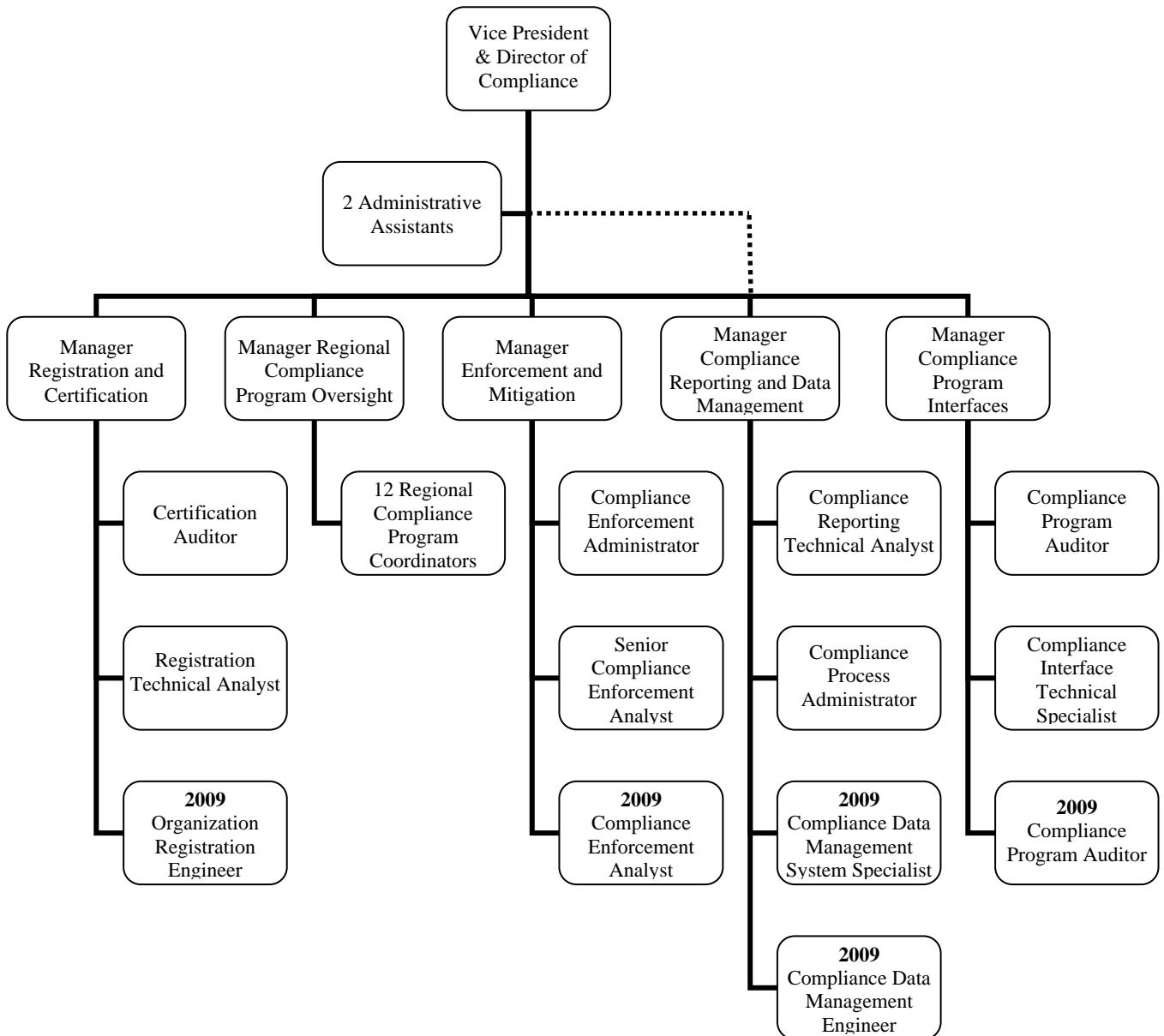
- Promote the reliability of the bulk power system through rigorous compliance monitoring and enforcement activities
- Facilitate uniformity of compliance activities throughout North America
- Improve the compliance program by analyzing compliance monitoring experience across North America and implementing necessary improvements

In 2009, NERC, the Regional Entities and the users, owners and operators of the bulk power system will have over 18 months of experience with the CMEP implementation. On-going monitoring, auditing, tracking of performance and identifying deficiencies in the program are resulting in process improvements at NERC, Regional Entities and Registered Entities. NERC will continue to resolve deficiencies and improve the program consistent with the rules on an ongoing basis.

⁴ CMEP Section 4.2: http://www.nerc.com/files/Appendix4C_Uniform_CMEP_10162007.pdf#page=31

3. NERC Compliance Monitoring and Enforcement Program Organization

NERC’s CMEP is implemented by the NERC Compliance Department and is organized into five (5) strategic areas. The five areas include registration and certification, compliance program interfaces (this area includes Regional Entity program audits), Regional compliance program oversight, enforcement and mitigation, and compliance reporting and data management as shown in the organization chart below.



4. 2009 Program Implementation - Discovery

The NERC 2009 CMEP will include all regulatory authority approved Reliability Standards being subject to spot checks, compliance violation investigations and complaints. NERC and the Regional Entities developed a risk based criteria for determining the scope of 2009 compliance audits and self certifications. The risk based criteria will help compliance auditors focus on the Reliability Standards that if violated pose the highest risk to the reliability of the bulk power system.

4.1 Application of Discovery Methods under the CMEP

NERC and the Regional Entities have processes in place to implement all eight compliance monitoring methods as appropriate. In 2009, the following will be implemented:

4.1.1 Compliance Audit and Self Certification

Requirements have been selected based on risk to the reliability of the bulk power system for inclusion in the 2009 compliance audits and self certifications. The risk based criteria includes Reliability Standard requirements that have been identified:

- With a high Violation Risk Factor⁵
- In the NERC top 10 list of allegedly violated Reliability Standards
- In past events and major reliability issues
- As a regional variation (*This will be a Regional Entity specific selection.*)
- As cyber security Reliability Standards (*All requirements in Critical Infrastructure Protection (CIP) Reliability Standards.*)
- In the audited entity's past performance (*This will be an audited entity-specific addition to the audit scope.*)
- As a result of a Registered Entity increasing its compliance responsibility due to mergers or acquisitions (*This will be an audited entity-specific addition to the audit scope.*)

NERC identified forty-nine (49) specific Reliability Standards including four-hundred eighteen (418) requirements for 2009 compliance audits and self certifications. In addition, NERC identified three (3) additional Reliability Standards including an

⁵ "Each requirement set out within NERC's Reliability Standards has been assigned a Violation Risk Factor (VRF) through the NERC Reliability Standards development process. The factors have been defined and approved through the standards development process and are assigned to requirements to provide clear, concise and comparative association between the violation of a requirement and the expected or potential impact of the violation to the reliability of the bulk power system. One of three defined levels of risk is assigned to each standards requirement: Lower Risk Factor, or; Medium Risk Factor, or; High Risk Factor. Definitions of the factors can be found in appropriate standards development process documentation." Rules of Procedure Paragraph 4.1.1 at the link: <http://www.nerc.com/page.php?cid=1|8|169>

additional one-hundred thirty (130) requirements for self certifications.⁶ See the 2009 CMEP Reliability Standard spreadsheet posted on the NERC Web site at the following link: http://www.nerc.com/files/2009_CMEP_Reliability_Standards.xls.

Additions to Compliance Audit Scope

- All ongoing and completed Mitigation Plans will be included in the compliance audit scope. Regional Entities must provide the Mitigation Plan status to the compliance audit team including documentation and evidence of validation for completed Mitigation Plans.
- Regional Entities have the authority to expand the audit scope based on regulatory authority approved Regional Entity Reliability Standards, the Registered Entity's past performance and other factors that impact the risk to reliability of the bulk power system.

4.1.2 2009 Compliance Audit Schedule

The 2009 compliance audit schedule is posted on the NERC Web site.⁷ This posted schedule is updated on a monthly basis, as necessary. The initial 2009 compliance audit schedule was initially posted in August 2008. This will be the ongoing process for posting audit schedules. This process allows 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. Both on-site and off-site audits are compliance audits and are performed via the same process. The only difference is logistics. Registered Entities performing the Reliability Coordinator, Balancing Authority and Transmission Operator functions must be audited on-site. The NERC Rules of Procedure Section 403, Paragraph 11.2 states: "Audits of bulk power system owners and operators with primary reliability responsibility will be performed on the audited entity's site. For other bulk power system users, owners, and operators on the NERC Compliance Registry, the audit may be either an on-site audit or based on review of documents, as determined to be necessary and appropriate by NERC or Regional Entity compliance program staff."

4.1.3 Semi-Annual Self Certifications for CIP-002-1 through CIP-009-1 Reliability Standards

The CIP-002-1 through CIP-009-1 Reliability Standards are regulatory approved Reliability Standards and are subject to enforcement in accordance with the NERC Guidance for Enforcement of CIP Standards⁸ and the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1.⁹

⁶ Two of the additional Reliability Standards identified for self certification are CIP-005-1 and CIP-006-1 (see section 4.1.2 of this Implementation Plan). The third additional Reliability Standard identified for self certification is TPL-004-0 (see section 4.2, Table 2 of this Implementation Plan).

⁷ <http://www.nerc.com/commondocs.php?cd=3>

⁸ http://www.nerc.com/files/Guidance_on_CIP_Standards.pdf

⁹ http://www.nerc.com/files/Guidance_on_CIP_Standards.pdf#page=5

FERC Order No. 706 P 96 states the ERO will conduct semi-annual self certifications prior to the date by which full compliance is required.¹⁰ NERC and the Regional Entities began conducting the semi-annual self certifications for all applicable Registered Entities identified in all Tables of the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 on July 1, 2008.

These self certifications will continue in 2009 with reporting dates of January 1, 2009 and July 1, 2009. NERC expects the Regional Entities to collect self certifications from all applicable Registered Entities identified in all Tables of the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 on July 1, 2008 regardless of the enforcement status of CIP-002-1 through CIP-009-1 requirements.

4.1.4 Spot Check

In 2009, NERC is requiring the Regional Entities perform spot checks for 13 requirements in CIP-002-1 through CIP-009-1 that will be classified as “Auditably Compliant” for specific functions identified in Table 1¹¹ of the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1.

These spot checks will begin July 1, 2009 going forward into 2010 until all applicable Registered Entities in Table 1¹¹ of the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1 are assessed for compliance. These spot checks can occur during a regularly scheduled compliance audit or as a separate activity.

All regulatory authority approved Reliability Standards are subject to spot checks. Spot checks for additional Reliability Standards have been identified by NERC as detailed in the 2009 CMEP Reliability Standards spreadsheet.¹² The Regional Entities can determine if all applicable entities or a representative sample of applicable entities will undergo the additional spot checks for the following Reliability Standards:

- **EOP-009-0** – Documentation of Blackstart Generating Unit Test Results
- **FAC-013-1** – Establish and Communicate Transfer Capabilities
- **IRO-014-1** – Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators
- **PRC-010-0** – Assessment of the Design and Effectiveness of UVLS Program
- **PRC-011-0** – UVLS System Maintenance and Testing
- **TOP-003-0** – Planned Outage Coordination

The Regional Entities can expand the list of Reliability Standards and requirements identified for spot checks they plan to perform as defined in their regional implementation plans.

¹⁰ http://www.nerc.com/files/Order_706.pdf#page=34

¹¹ http://www.nerc.com/files/Guidance_on_CIP_Standards.pdf#page=6

¹² http://www.nerc.com/files/2009_CMEP_Reliability_Standards.xls

4.1.5 Periodic Data Submittals

Specific Reliability Standards and requirements have been identified for periodic data submittals. In 2009, NERC is requiring periodic data submittals from the Registered Entities to the Regional Entities for the following Reliability Standards:

- **BAL-001-0a** – Real Power Balancing Control Performance
- **BAL-002-0** – Disturbance Control Performance (DCS)
- **BAL-003-0a** – Frequency Response and Bias
- **BAL-006-1** – Inadvertent Interchange
- **FAC-003-1** – Transmission Vegetation Management Program
- **PRC-004-1** – Analysis and Mitigation of Transmission and Generation Protection System Misoperations
- **PRC-016-0** – Special Protection System Misoperations
- **PRC-021-1** – Under-Voltage Load Shedding Program Data
- **TPL-001-0** – System Performance Under Normal Conditions
- **TPL-002-0** – System Performance Following Loss of a Single BES Element
- **TPL-003-0** – System Performance Following Loss of Two or More BES Elements
- **TPL-004-0** – System Performance Following Extreme BES Events

More specific information regarding periodic data submittals will be defined in the regional implementation plans.

4.1.6 Exception Reporting

Specific Reliability Standards and requirements in the 2009 CMEP Reliability Standard spreadsheet¹³ have been identified for exception reporting. In 2009, NERC is requiring exception reporting from the Registered Entities to the Regional Entities for the following Reliability Standards:

- **BAL-003-0a** – Frequency Response and Bias
- **BAL-004-0** – Time Error Correction
- **BAL-006-1** – Inadvertent Interchange
- **EOP-004-1** – Disturbance Reporting
- **EOP-006-1** – Reliability Coordination - System Restoration
- **INT-001-3** – Interchange Information

¹³ http://www.nerc.com/files/2009_CMEP_Reliability_Standards.xls

- **INT-003-2** – Interchange Transaction Implementation
- **INT-004-2** – Dynamic Interchange Transaction Modifications
- **IRO-004-1** – Reliability Coordination - Operations Planning
- **IRO-015-1** – Notifications and Information Exchange between Reliability Coordinators
- **IRO-016-1** – Coordination of Real-time Activities between Reliability Coordinators
- **PER-003-0** – Operating Personnel Credentials
- **TOP-005-1** – Operational Reliability Information
- **TOP-007-0** – Reporting SOL & IROL Violations Evaluation
- **VAR-002-1a** – Generator Operation for Maintaining Network Voltage Schedules

The CMEP Section 3.7¹⁴ states: “The Compliance Enforcement Authority shall also require Registered Entities to confirm the number of exceptions that have occurred in a given time period identified by NERC, even if the number of exceptions is zero.” More specific information regarding exception reporting submittals will be defined in the Regional Implementation Plans.

4.1.7 Compliance Violation Investigation

All regulatory authority approved Reliability Standards are subject to a compliance violation investigation. The CMEP Section 3.4 states: “A Compliance Violation Investigation may be initiated at any time by the Compliance Enforcement Authority, NERC, FERC or another Applicable Governmental Authority in response to a system disturbance, Complaint, or possible violation of a Reliability Standard identified by any other means.”¹⁵

4.1.8 Self Report

Registered Entities can self report compliance violations with any regulatory authority approved Reliability Standard. Self reports of compliance violations must go through the appropriate Regional Entity. NERC strongly encourages Registered Entities to report violations of Reliability Standards as soon as possible to the appropriate Regional Entity.

¹⁴ http://www.nerc.com/files/Appendix4C_Uniform_CMEP_10162007.pdf#page=28

¹⁵ http://www.nerc.com/files/Appendix4C_Uniform_CMEP_10162007.pdf#page=20

4.1.9 Complaint

All regulatory authority approved Reliability Standards or requirements are subject to a complaint regarding a compliance violation by a Registered Entity.

NERC maintains a Compliance Hotline to receive complaints. Any person may submit a complaint to report a possible violation of a Reliability Standard by completing the form on <https://www.nerc.net/hotline/>. If so requested, NERC and Regional Entity staff will withhold the name of the complainant in any communications with the alleged violating entity. All information provided will be held as confidential in accordance with the NERC Rules of Procedure.¹⁶ The compliance staff will informally seek additional information from the submitter and others, as appropriate. The compliance staff may refer the matter for further investigation by NERC or the appropriate Regional Entity.

Complaints may also be made via phone by calling 609-524-7069 or by sending an e-mail directly to hotline@nerc.net.

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

4.2 Reliability Standards Subject to 2009 CMEP Implementation

2009 is the first year in the CMEP in which all regulatory authority approved Reliability Standards and requirements are identified in the program.

All regulatory authority approved Reliability Standards and requirements are subject to a compliance audit, spot check, self report, self certification, compliance violation investigation and complaint. As mentioned in section 4.1 of this Implementation Plan, NERC and the Regional Entities developed risk based criteria for determining the scope of 2009 compliance audits and self certifications. The risk based criteria will help compliance auditors focus on the Reliability Standards that if violated pose the highest risk to the reliability of the bulk power system. This approach is new and is in the early stages of development. Because of this, NERC will use the definition of actively monitored requirements in the Rules of Procedure for identifying the minimum scope of compliance audits and self certifications in 2009.

The NERC Rules of Procedure,¹⁷ Section 401 - Scope of the NERC Compliance Enforcement Program, Paragraph 6, defines Actively Monitored Requirements as:

“Actively Monitored Requirements — NERC, with input from the Regional Entities, stakeholders, and regulators, shall annually select a subset of the NERC Reliability Standards and requirements to be actively monitored and audited in the NERC annual compliance program. Compliance is required with all NERC Reliability Standards whether or not they are included in the subset of Reliability Standards and requirements

¹⁶ <http://www.nerc.com/page.php?cid=1|8|169>

¹⁷ http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20080321.pdf#page=25

designated to be actively monitored and audited in the NERC annual compliance program.”

All Reliability Standards and requirements identified in the 2009 program are listed in the 2009 CMEP Reliability Standard spreadsheet posted on the NERC Web site at the following link: http://www.nerc.com/files/2009_CMEP_Reliability_Standards.xls. This spreadsheet includes the following Tabs:

- **Summary Tab:** A quick reference listing of the Reliability Standards and requirements identified for compliance audits, self certifications and spot checks required by NERC in 2009. This tab is designed to give the user a quick reference of the lists. There are also comparisons of the number of Reliability Standards and requirements monitored in the 2007, 2008 and 2009 programs.
- **Reliability Standards Detail Tab:** Provides a detailed list of the Reliability Standards included in the 2009 CMEP. Also provides the risk based criteria for identifying Reliability Standards determined in the minimum scope of compliance audits and self certifications.
- **Requirements Detail Tab:** Provides a detailed list of the requirements included in the 2009 CMEP. Also provides the risk based criteria for identifying requirements determined in the minimum scope of compliance audits and self certifications.
- **Top 10 Standards AV Tab:** This tab lists the top 10 Reliability Standards and associated requirements allegedly violated June 2007 through June 2008. This information was used in the risk based criteria for identifying Reliability Standards and requirements for compliance audits and self certifications in 2009.
- **Revision History:** The 2009 CMEP Reliability Standards spreadsheet will be a dynamic document and as Reliability Standards and requirements change and as new Reliability Standards and requirements are approved by applicable governmental authorities, the spreadsheet will be updated. The revision history will allow users, owners and operators of the bulk power system to see all of the changes during the year. NERC compliance will issue announcements to Registered Entities when this spreadsheet changes.

The 2009 CMEP Reliability Standards spreadsheet also identifies which Reliability Standards and requirements were included in the 2007 and 2008 Compliance Monitoring and Enforcement Programs. This information is important to track because the NERC CMEP¹⁸ Section 3.1.4 Scope of Compliance Audits states:

“A Compliance Audit will include all Reliability Standards applicable to the Registered Entity monitored in the NERC Implementation Plans in the current and three previous years, and may include other Reliability Standards applicable to the Registered Entity. If a Reliability Standard does not require retention of data for the full period of the

¹⁸ <http://www.nerc.com/commondocs.php?cd=3>

Compliance Audit, the Compliance Audit will be applicable to the data retention period specified in the Reliability Standard.”

The compliance audit scope (using the risk based criteria and the data retention listed in specific standards and requirements) in the 2009 CMEP Implementation Plan will result in fewer Reliability Standards than in the 2008 CMEP Implementation Plan. In order to address gaps in the 2009 vs. 2008 compliance audit scopes, alternative compliance monitoring methods are proposed in Table 1 below. Addressing the gaps between the 2008 and 2009 programs for compliance audit scope is necessary to justify any deviations from the CMEP Section 3.1.4.

Table 1: Alternatives to Address Gaps between 2008 and 2009 CMEP Audit Scopes

Reliability Standard	Proposed Alternative to Compliance Audit	Justification
BAL-001-0a – Real Power Balancing Control Performance	<ul style="list-style-type: none"> • Monthly Data Submittals 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low, • This standard was not in the top 10 allegedly violated list
BAL-003-0a – Frequency Response and Bias	<ul style="list-style-type: none"> • Annual Data Submittals • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
BAL-004-0 – Time Error Correction	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low • This standard was not in the top 10 allegedly violated list
BAL-006-1 – Inadvertent Interchange	<ul style="list-style-type: none"> • Monthly Data Submittals • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low • This standard was not in the top 10 allegedly violated list
EOP-004-1 – Disturbance Reporting	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list • Event driven standard
EOP-009-0 – Documentation of Blackstart Generating Unit Test Results	<ul style="list-style-type: none"> • Spot Check 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
FAC-013-1 – Establish and Communicate Transfer Capabilities	<ul style="list-style-type: none"> • Spot Check 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Medium • This standard was not in the top 10 allegedly violated list

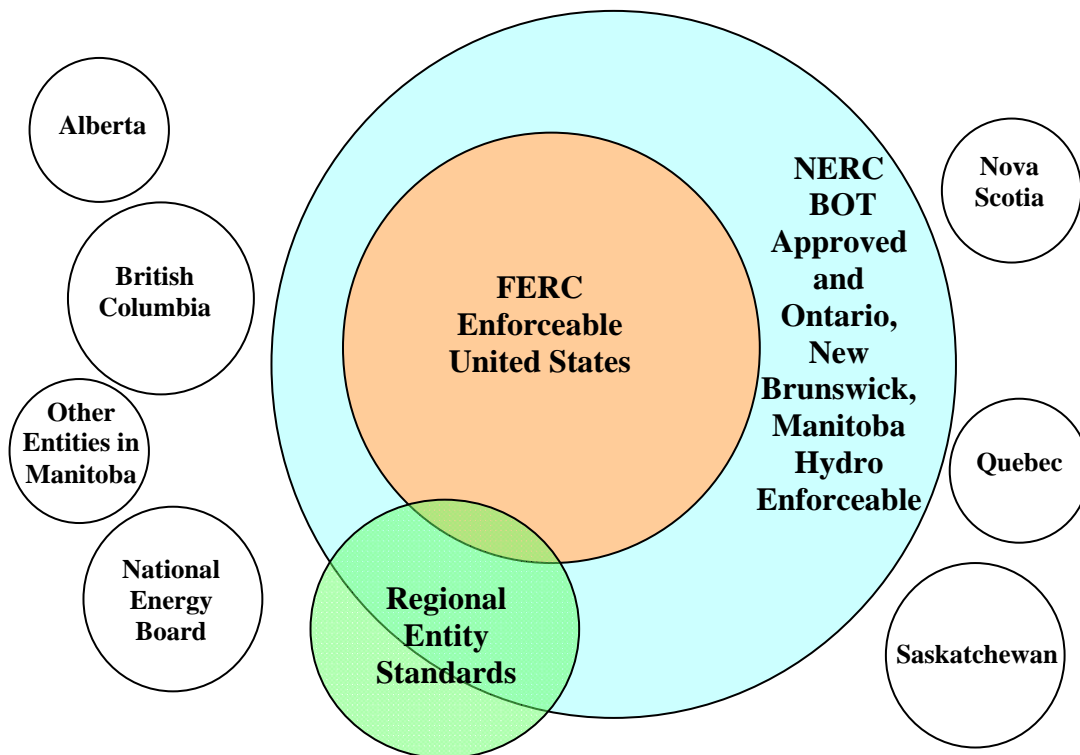
Reliability Standard	Proposed Alternative to Compliance Audit	Justification
INT-001-3 – Interchange Transaction Tagging	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low • This standard was not in the top 10 allegedly violated list
INT-003-2 – Interchange Transaction Implementation	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
INT-004-2 – Interchange Transaction Modifications	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low • This standard was not in the top 10 allegedly violated list
IRO-014-1 – Procedures, Processes, or Plans to Support Coordination Between Reliability Coordinators	<ul style="list-style-type: none"> • Spot Check 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
IRO-015-1 – Notification and Information Exchange Between Reliability Coordinators	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
IRO-016-1 – Coordination of Real-Time Activities Between Reliability Coordinators	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
PRC-010-0 – Assessment of the Design and Effectiveness of UVLS Program	<ul style="list-style-type: none"> • Spot Check 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
PRC-011-0 – UVLS System Maintenance and Testing	<ul style="list-style-type: none"> • Spot Check 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
PRC-016-0 – Special Protection System Misoperations	<ul style="list-style-type: none"> • Periodic Data Submittals 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Medium • This standard was not in the top 10 allegedly violated list
PRC-021-1 - Under-Voltage Load Shedding Program Data	<ul style="list-style-type: none"> • Annual Data Submittal 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list

Reliability Standard	Proposed Alternative to Compliance Audit	Justification
TOP-003-0 – Planned Outage Coordination	<ul style="list-style-type: none"> • Spot Check 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Medium • This standard was not in the top 10 allegedly violated list
TOP-005-1 – Operational Reliability Information	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
TPL-004-0 – System Performance Following Extreme BES Events	<ul style="list-style-type: none"> • Self Certification 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list
VAR-002-1a - Generator Operation for Maintaining Network Voltage Schedules	<ul style="list-style-type: none"> • Exception Reporting 	<ul style="list-style-type: none"> • The VRFs for the requirements in this standard are Low/Medium • This standard was not in the top 10 allegedly violated list

5. 2009 Program Implementation - Enforcement

Enforcement of Reliability Standards varies throughout North America. In the United States, FERC approved Reliability Standards became mandatory and enforceable on June 18, 2007. The Canadian Jurisdictions enforcement status is listed in Appendix C of the NERC 2007 CMEP Annual Report.¹⁹ Currently, NERC Reliability Standards are mandatory in New Brunswick, Ontario and Manitoba Hydro. Figure 1 is a Venn diagram displaying the NERC Reliability Standards enforcement status in North America.

Figure 1: NERC Enforceable Reliability Standards in North America



5.1 Violation Reporting

The process for reporting violations of Reliability Standards from the Regional Entities to NERC is continuously improving. Section 8.0 Reporting and Disclosure of the Compliance Monitoring and Enforcement Program specifies that violations of Reliability Standards must be reported to NERC by the Regional Entity within 5 business days. In 2008 the Regional Entities routinely reported violations to NERC in less than 5 business days and in many cases, the violations are reported within 2 business days.

In 2004, NERC began identifying a list of Reliability Standards that, if violated, the regions had to report the violation to NERC within 48 hours of becoming aware of the

¹⁹ <http://www.nerc.com/page.php?cid=3|26>

violation.²⁰ This legacy practice has continued through 2008. Because of the reporting process improvements since 2004 and the fact that all violations are now reported to NERC in less than 5 business days and in most cases within 2 business days, the need to specify a static list of 48-hour reporting Reliability Standards is no longer necessary. NERC, instead, is encouraging the Regional Entities to consistently incorporate other proactive methods of identifying and mitigating risk to reliability of the bulk power system. One of these methods is the Remedial Action Directive.

5.2 Remedial Action Directives

Remedial Action Directives²¹ are used to address imminent threats to reliability of the bulk power system. Regional Entities must notify NERC within 2 business days after issuing a Remedial Action Directive. Regional Entities should consult with NERC prior to issuing a Remedial Action Directive.

Note: A Remedial Action Directive is not a substitution for penalties.

5.3 Mitigation Plan Approvals

Mitigation plans are a critical part of improving bulk power system reliability and Registered Entities must develop and follow Mitigation Plans to not only mitigate the compliance violations, but to also prevent reoccurrence of the compliance violations.

The CMEP, Section 6.2 - Contents of Mitigation Plans, includes a list of specific information that must be part of a Mitigation Plan. Based on lessons learned regarding Mitigation Plans received, including Mitigation Plans for the pre-June 18, 2007 self reported compliance violations, NERC developed an accompanying list of criteria to help the Regional Entities proactively resolve unacceptable Mitigation Plans with Registered Entities before the Mitigation Plans are submitted to NERC for approval. Table 2 in Appendix A includes columns for: (i) identification of some key Mitigation Plan components and (ii) NERC expectations of the Mitigation Plans with respect to those components. Please note that the expectations provided in Table 2 are illustrative, only, of things that NERC wishes to highlight at this time; they are not limitations to NERC in its assessment of any given Mitigation Plan. Table 2 must be used in conjunction with Section 6.2 of the CMEP.

Each Regional Entity shall include in its Regional Implementation Plan, actions to be taken if Mitigation Plans for violations that pose a high risk to the reliability of the bulk power system are not completed by the Registered Entity.

5.4 Regional Entity Validation of Completed Mitigation Plans

²⁰ See the NERC 2004 Compliance Enforcement Program Annual Report at the following link: http://www.nerc.com/files/Final_2004_CEP_Report.pdf#page=8.

²¹ The Compliance Monitoring and Enforcement Program defines a Remedial Action Directive as: Remedial Action Directive: An action (other than a penalty or sanction) required by a Compliance Enforcement Authority that (1) is to bring a Registered Entity into compliance with a Reliability Standard or to avoid a Reliability Standard violation, and (2) is immediately necessary to protect the reliability of the bulk power system from an imminent threat.

NERC expects each Regional Entity to validate the completion of Mitigation Plans by assessing evidence of compliance provided by the Registered Entity either on-site or submitted to the Regional Entity office. The Mitigation Plan validations will be conducted in the same manner as the compliance assessment process used for the eight compliance discovery methods. This compliance assessment process must be executed by NERC trained Regional Entity staff using NERC compliance assessment guides such as Reliability Standard Audit Worksheets (RSAWs). The Mitigation Plan validation process and documentation must be retained for review by NERC.

The CMEP Section 6.7 states: “Regional Entities will provide to NERC the quarterly status reports and such other information as NERC requests, and will notify NERC when each Mitigation Plan is verified to have been completed.”²²

²² http://www.nerc.com/files/Appendix4C_Uniform_CMEP_10162007.pdf#page=41

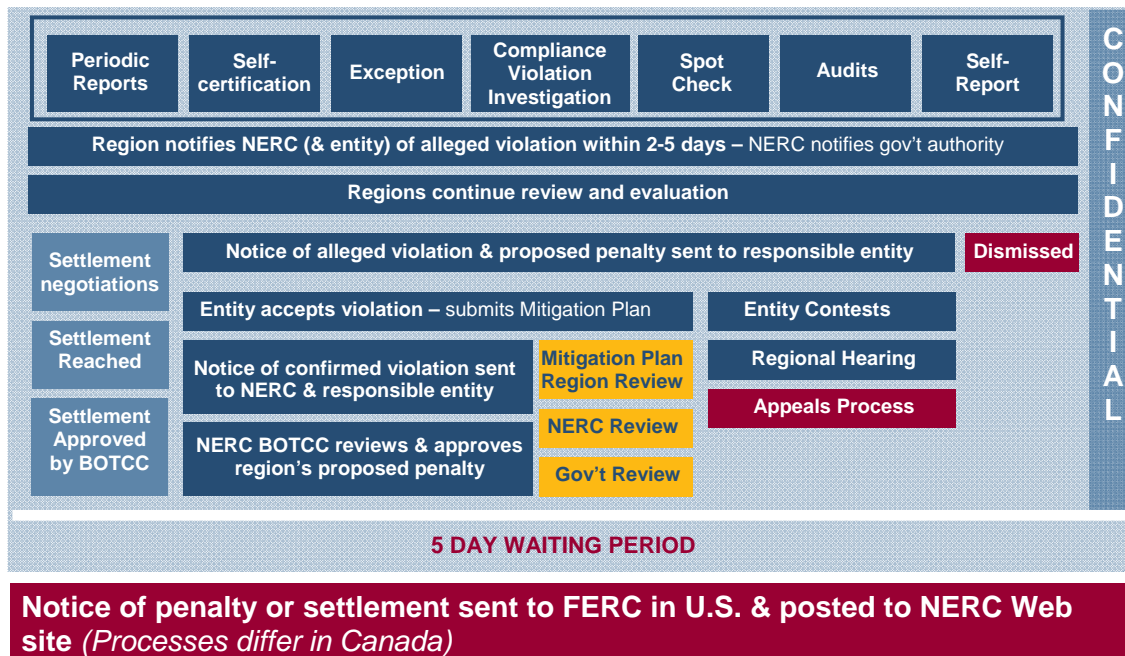
6. Improving Transparency and Consistency

NERC and the Regional Entities receive CMEP implementation feedback from the Compliance and Certification Committee and other stakeholders. All feedback and input from these groups, among others, is reviewed on a continuous basis for opportunities for improvement. NERC and the Regional Entities are committed to continuous improvement of the CMEP implementation in these formative years of the program. Updates on the status of actions taken in response to stakeholder feedback are described in the sections below.

6.1 Improve Transparency of the CMEP Implementation

NERC and the Regional Entities are attempting to balance the request from the industry to improve transparency with the confidential nature of the CMEP processes. Figure 2 is a pictorial view of the compliance process and shows how most of the processes in the CMEP fall under a window of confidentiality. Despite the confidential caveat, NERC and the Regional Entities are continuously identifying and implementing innovative ways to share CMEP process information while honoring confidentiality.

Figure 2: Compliance Process²³



²³ Note: Complaints are processed through one of the other 7 compliance monitoring methods.

6.1.1 Yearly Compliance Audit Schedules

NERC posts the yearly compliance audit schedules on its Web site at the following link: <http://www.nerc.com/commondocs.php?cd=3>. In 2008, NERC and the Regional Entities agreed to update this schedule on a monthly basis. Other improvements made to the schedule since 2007 include: 1) adding the NERC Registration ID number and 2) identifying the NERC staff participating on the audit team. The 2008 audit schedule was not posted until early January 2008. Instead of waiting until the Regional Entities have firm dates for the compliance audits, initial schedules for the upcoming year will begin to be posted on the NERC Web site in August. This schedule will also be updated monthly.

6.1.2 Status of Compliance Audit Reports

The CMEP states that compliance audit reports will be posted on the NERC Web site. If the compliance audit report contains findings of compliance with all Reliability Standards and requirements reviewed during the compliance audit then NERC will post the compliance audit report on its public Web site. If a compliance audit report contains findings of possible violations, NERC will not post the compliance audit report until all possible violation findings go through due process. Once due process has occurred, the Regional Entity will submit a public version of the compliance audit report and a procedural summary listing the outcome of the possible violation findings. This package containing the procedural summary and the compliance audit report will be posted on the NERC public Web site.

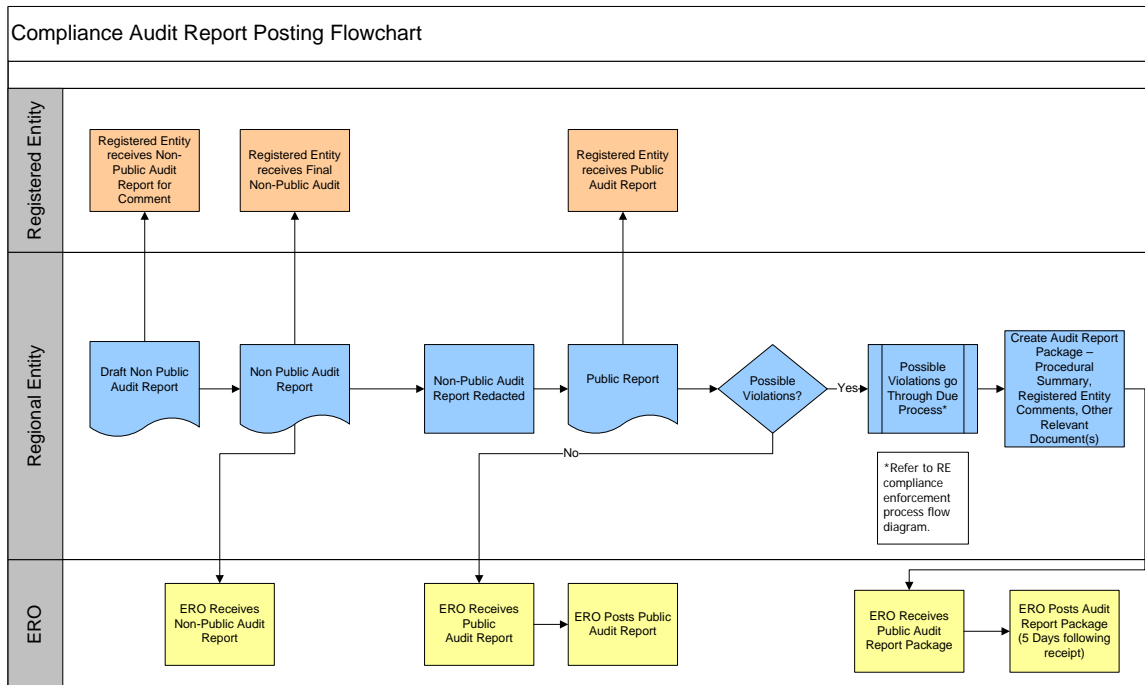
NERC added a column to the yearly compliance audit schedules called audit reports. The compliance audit report status is indicated in the audit report column as follows:

Compliance Audit Report Status Definitions:

- **Received:** NERC has received a copy of the final compliance audit report.
- **Received - Posted:** NERC has received a copy of the final compliance audit report and has posted it on the NERC public Web site at the following link.

<http://www.nerc.com/page.php?cid=3|26|246>

Displaying the compliance audit report status on the NERC public Web site has resulted in NERC and the Regional Entities being more diligent in promptly completing the compliance audit reports. Figure 3 below shows the compliance audit report posting flowchart.

Figure 3: Compliance Audit Report Posting Flowchart

6.1.3 Reliability Standard Audit Worksheet²⁴

The NERC Reliability Standard Audit Worksheets are designed to add clarity and consistency to the audit team's assessment of compliance with Reliability Standards. Comments on these and any of NERC's auditor resources are welcome and can be directed to the Regional Entity Compliance Managers. For more information on NERC's regional programs, please *see* the following link:

<http://www.nerc.com/page.php?cid=3|23>.

The RSAWs are posted on the NERC public Web site and provide information to the industry about types of evidence required to show compliance with a Reliability Standard. This information is updated as needed to ensure the latest information about the application of a Reliability Standard.

Additional information will be added to the RSAWs in preparation for the 2009 CMEP implementation. This information includes: 1) adding excerpts from FERC Orders regarding the application or intent of a Reliability Standard requirement, 2) updating the disclaimer statement on the RSAWs, 3) adding all consensus auditing practices agreed to by NERC and the Regional Entities, 4) adding NERC guidance for particular requirements to ensure consistency of audit approach, and 5) consolidating the RSAW and the pre-audit questionnaire into one document. As these documents are combined for each Reliability Standard, the new documents will be posted on the auditor resources Web site.

²⁴ The RSAWs are posted on the NERC public website at the following link: <http://www.nerc.com/page.php?cid=3|22>.

6.2 Multiple Region Registered Entities (MRRE)

NERC is working with the Regional Entities in 2008 to develop a MRRE coordination process. This process will prevent duplication of effort by multiple regions to assess compliance for MRREs. More information about MRRE coordination will be shared as the process is developed.

6.3 Provide Feedback to the NERC Reliability Standards Development Process

NERC and the Regional Entities understand the need to provide feedback to the Reliability Standards Development Process. In 2008, the Regional Entity Compliance Managers submitted a request for a formal interpretation of EOP-001, R1. The initial ballot results for the interpretation for EOP-001, Requirement 1, "Emergency Operations Planning," have been posted.²⁵

Other activities involving feedback to the Reliability Standards Development Process are being conducted through recommendations from NERC Compliance on auditing approaches for Reliability Standard requirements.

The compliance interfaces group is leading the effort to develop and update Compliance Elements in the Reliability Standards.

These activities will continue in 2009.

6.4 Provide Information to the Industry about the CMEP

In June 2008, NERC began announcing to compliance contacts in the Registration Database²⁶ about new information regarding the CMEP implementation on the NERC public Web site. The following list includes the type of updates being announced to Registered Entities:

- Updates or new postings of RSAWs
- Monthly update of the yearly compliance audit schedule(s)
- New compliance reports or policy documents
- Requests for industry comment/surveys
- Notice of Penalty filings
- Updated Q&A reports
- Compliance guidance documents
- Compliance Job Aids

7. 2009 Regional CMEP Implementation Plans

²⁵ http://www.nerc.com/filez/standards/EOP-001-0_ Interpretation_RECM.html

²⁶ See the NERC Compliance Registry at the following link: <http://www.nerc.com/page.php?cid=3|25>

The Regional Implementation Plan is defined in the NERC CMEP as follows:

“An annual plan, submitted by November 1 of each year to NERC for approval that, in accordance with NERC Rule of Procedure Section 401.6 and the NERC Compliance Monitoring and Enforcement Program Implementation Plan, identifies (1) all Reliability Standards identified by NERC to be actively monitored during each year, (2) other Reliability Standards proposed for active monitoring by the Regional Entity, (3) the methods to be used by the Regional Entity for reporting, monitoring, evaluation, and assessment of performance criteria with each Reliability Standard, and (4) the Regional Entity’s Annual Audit Plan.”

NERC expects the Regional Entities to include all of the items listed in the Regional Implementation Plan definition above. In particular, NERC expects the following in addition to directives stated in other sections of this Implementation Plan:

1. All Reliability Standards identified by NERC in the 2009 CMEP Reliability Standards spreadsheet.²⁷
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 2009 CMEP Reliability Standards spreadsheet. For compliance audits, if the audit scope for a Registered Entity expands beyond the NERC 2009 CMEP Reliability Standards spreadsheet, the Regional Entity must notify the Registered Entity of the expanded audit scope and reasons for the expansion. For references to NERC guidance or implementation plans such as the CIP Guidance, a link should be included in the regional implementation plan instead of listing the entire document.
4. The Regional Entity’s Annual Audit Plan. The new process of providing a 2009 compliance audit schedule beginning in August 2008 should be referenced in the Regional Implementation Plan. There is no need to provide a schedule in the implementation plan other than the list of Registered Entity names, NERC Registration ID, and the year they will be audited. The Regional Entity can provide its audit plan for multiple years in the future.

Appendix A – Mitigation Plan Table

²⁷ http://www.nerc.com/files/2009_CMEP_Reliability_Standards.xls

Table 2: Mitigation Plan Table²⁸

Mitigation Plan (MP) Component	NERC Expectation
Description of Violation(s)	<p>The entity's statement must include:</p> <ol style="list-style-type: none"> 1. Identify the specific requirements of the standard consistent with the violations the Compliance Enforcement Authority (CEA) has alleged or confirmed, as applicable. 2. Describe how each of these requirements was allegedly violated. 3. The descriptions must be consistent with CEA's understanding and description of how the requirements were allegedly violated.
Registered Entity's Plan to prevent recurrence of the alleged or confirmed violations	<ul style="list-style-type: none"> ▪ Requiring mitigation of a violation by an entity is an aspect of the overall sanctioning of that entity by the CEA for that violation.²⁹ ▪ In light of the above a key goal of every ERO-approved Mitigation Plan, as an element of the CEA's sanctioning of the associated violation(s), must also to be proactive regarding future violations of the same or any other Reliability Standard, particularly ones that are similar to the one violated. For instance, the CEA's goal with an entity that has incurred a violation for failure to have documentation required for one standard, should be to prompt review, and correction if necessary, by the subject entity that it has acceptable documentation for all other standards it is responsible for. ▪ Accordingly acceptable completion of this part of the MP form is required even where the MP has been completed and the form is being completed and submitted as a matter of record.
Registered Entity Point of Contact	<p>CMEP Section 6.2 states Point of Contact must be:</p> <ol style="list-style-type: none"> 1. Responsible for filing the MP. 2. Technically knowledgeable regarding the MP. 3. Authorized & competent to respond to questions regarding the status of the MP.

²⁸ This Mitigation Plan table is to be used in conjunction with Section 6.2 of the CMEP.

²⁹ In general sanctioning an entity for incurring a violation is intuitively recognized as penal and reactive because it is assessed (i) after the violation has occurred and (ii) directly in response to the violation. However, effective sanctioning (*i.e.* that which also discourages or prevents other or additional violations by the entity or others and thereby supports the goals of the sanctioning authority) is only achieved where the sanctioning is also proactive and illustrative/educational regarding the authority's requirements and expectations.

Mitigation Plan (MP) Component	NERC Expectation
Ensure reliability during the implementation of the MP	<ul style="list-style-type: none"> ▪ Like acceptable completion of the section of the MP addressing protection against future occurrences of violations this part of the MP must generally be completed and always be acceptable (<i>i.e.</i> completed or not completed, and content) to the CEA and NERC. ▪ Generally speaking, this section of the MP form may be left uncompleted by the entity where the entity indicates it has already completed the plan prior to submitting it. <u>However, a MP is not fully completed until the CEA has verified completion; therefore it is within the CEA's or NERC's authority, and within either's discretion, to require that the entity continue operations etc under some restriction until completion of the MP is verified.</u> ▪ It may be acceptable that the entity is taking no additional actions beyond directly addressing the violations through the MP while implementing the plan.
Timetable for completion of the MP	<p>MP Completion date: This must be provided and understood by the entity as the date that the entity is proposing, and committing to, that its proposed plan will be completed and after which it understands additional sanctioning will be assessed by the RE or NERC if the plan is not complete.³⁰</p> <p>Timeliness of MP Completion date: The fact that there are one or more violations to be mitigated by the MP proposed implies that the reliability of the BPS is bearing - and BPS Users owners and operators are having to manage - some additional risk until the MP is complete and verified. As with all enforcement matters NERC expects the CEA to be aggressive but reasonable with respect to how quickly the MP is to be completed.</p>
Implementation Milestones	Every proposed MP should include some milestones however plans with proposed durations of over 3 months must include them.
MP must directly address the violation	<ul style="list-style-type: none"> ▪ Consistent with requirements and expectations regarding description of the violation(s) the corrective action plan proposed by the entity must directly address the violation. ▪ The MP plan must be specific in how the entity plans to become compliant. ▪ Reasonable detail is expected at the "by requirement" level unless more aggregate grouping is reasonable and the CEA accepts same, with conditions if/as the CEA deems appropriate.
MP must have a suitable level of specificity and exactness	In addition to addressing each requirement directly the MP must also address each one at suitable levels of specificity and exactness.
MP must clearly indicate entity's commitment that violation(s) in question will be mitigated at completion of the plan	<ul style="list-style-type: none"> ▪ It is not acceptable that any MP be considered complete, and the subject entity off the hook for anything less than full compliance post-completion of the plan, until the violations addressed by it is fully mitigated. ▪ Accordingly it will unacceptable for the entity's commitment to any MP to be limited to anything less than full restitution of compliance with the associated violations.

³⁰ In the event that the entity will not establish a date acceptable to NERC and the Regional Entity then the Regional Entity or NERC can and may set the completion date for the plan through a compliance directive.