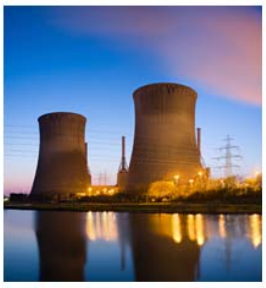
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2017 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan

Version 2.5

May 2017

RELIABILITY | ACCOUNTABILITY

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

Table of Contents

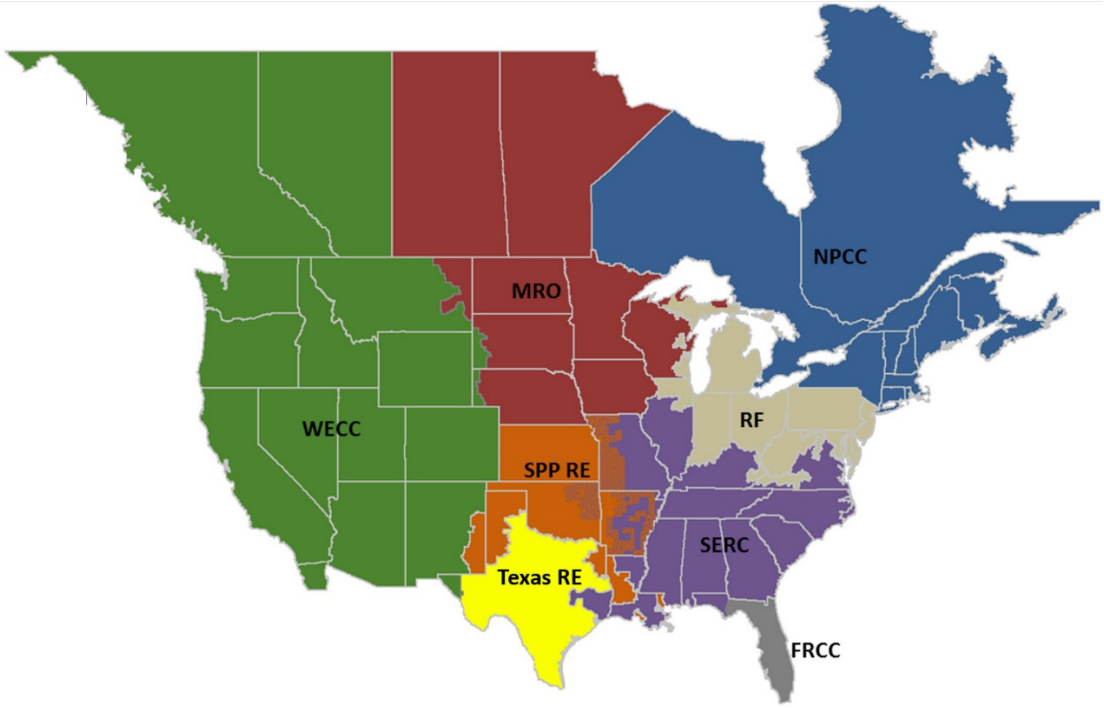
Revision History

Version	Date	Revision Detail
Version 1.0	September 14, 2016	• Release of the 2017 ERO CMEP Implementation Plan The ERO CMEP IP is the NERC portion only of the CMEP IP.
Version 2.0	November 30, 2016	• Release of the 2017 ERO Enterprise CMEP Implementation Plan. • The ERO Enterprise CMEP IP includes the Regional Entities' Implementation Plans within Appendix A.
Version 2.1	December 1, 2016	• Added Appendix B Compliance Assessment Report page 82. • Edited 'Registered Entity Responsibilities in CA Process' page 4.
Version 2.2	December 12, 2016	• Removed duplicates and added new registered entity in ReliabilityFirst Compliance Audit Plan.
Version 2.3	January 5, 2017	• Updated FRCC Compliance audit plan page 23 – removed CIP audits for City of Homestead and Gainesville.
Version 2.4	March 9, 2017	• Updated footnote 6 link on page 4. • Updated FRCC Fall Conference Workshop dates from November 14 -15 to November 7-8.
Version 2.5	May 17th, 2017	• Corrected header on page 4

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Introduction

Purpose

The Electric Reliability Enterprise (ERO) Enterprise Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) is the annual operating plan used out by Compliance Enforcement Authorities (CEAs) while performing their responsibilities and duties. CEAs, which consist of NERC and the eight Regional Entities (REs), execute CMEP activities in accordance with the NERC Rules of Procedure (ROP) (including Appendix 4C), their respective Regional Delegation Agreements, and other agreements with the Canadian regulatory authorities.

The ROP requires NERC to provide an IP to the REs on or about September 1 of the preceding year.[1] REs must submit their IPs to NERC for review and approval on or about October 1. RE IPs provide:

- Details on Regional Risk Assessment processes and results;
- Reliability Standards and Requirements associated with Regional Risk Assessment results;
- The RE compliance oversight plan, which includes the annual audit plan; and
- Other key activities and processes used for CMEP implementation.

The ERO Enterprise maintains a consolidated IP that provides guidance and implementation information common between NERC and the eight REs.

Implementation Plan

The ERO Enterprise consolidated IP uses a streamlined format that eliminates redundant information, improves transparency of CMEP activities, and promotes consistency among the RE-specific IPs. This format provides ERO Enterprise-wide guidance and implementation information while preserving RE differences by appending RE-specific IPs to supplement the overall ERO Enterprise IP. The RE-specific IPs describe risk assessments that identify the risks that the REs will consider as part of their compliance oversight plans.

NERC is responsible for collecting and reviewing the RE IPs to help ensure REs provide appropriate and consistent information regarding how they conduct CMEP activities. NERC monitors RE progress of CMEP activities against the RE IPs throughout the year and reports on CMEP activities in a year-end annual CMEP report.[2]

During the implementation year, NERC or an RE may update their portions of the IP. Updates may include, but are not limited to: changes to compliance monitoring processes; changes to RE processes; or updates resulting from a major event, FERC order, or other matter. REs submit updates to the NERC Compliance Assurance group, which reviews the updates and makes any needed changes. When changes occur, NERC posts a revised plan on its website and issues a compliance communication.

RE-specific IPs are due to NERC for review and approval on or about October 1. NERC will review the Regional specific IPs and include them in this document in Appendix A (1–8).

[1] NERC ROP, Section 403 (Required Attributes of RE Compliance Monitoring and Enforcement Programs).
[2] ERO Enterprise Annual CMEP Reports available at http://www.nerc.com/pa/comp/Pages/AnnualReports.aspx

Significant Initiatives Impacting CMEP Activities

The following ongoing NERC initiatives continuing in 2017 impact the ERO Enterprise's CMEP implementation.

Critical Infrastructure Protection (CIP) Reliability Standards, Version 5

Background

Similar to previous years, the ERO Enterprise is continuing its focus on protecting the Bulk Power System (BPS) against cyber security compromises that could lead to misoperation or instability. On November 22, 2013, Federal Energy Regulatory Commission (FERC) approved Version 5 of the Critical Infrastructure Protection (CIP) standards, which represent significant progress in mitigating cyber risks to the BPS and address all remaining cyber security-related FERC directives. On February 25, 2016, FERC issued a letter order granting an extension of time to defer the implementation of the CIP Version 5 Reliability Standards from April 1, 2016 to July 1, 2016 to align with the effective date for the revised CIP Reliability Standards approved in Order No. 822. NERC posted a spreadsheet containing effective dates of the CIP standards (with the exception of CIP-014-2) to clarify the mandatory and enforceable dates for cyber security requirements.

When FERC approved the first version of NERC's cyber security standards in 2008, it issued more than 100 directives for continued improvement. Since then, NERC and industry stakeholders have used a phased approach to develop modifications that address the directives, culminating in a FERC order directing NERC to address all remaining directives by March 31, 2013. NERC satisfied this order with CIP Version 5.

CIP Version 5 (CIP-002-5.1, CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5, CIP-009-6, CIP-010-2, and CIP-011-2) represents significant progress in mitigating cyber risks to the BPS, applying industry experience from earlier versions, and leveraging lessons learned from implementing and auditing entities for compliance with previous versions of the cyber security standards.

CIP Version 5 offers increased flexibility in implementing risk mitigation to individual entity operations, eliminates unnecessary documentation requirements, and transitions from the rigid "in or out" classification of previous versions to a more flexible "low-medium-high" impact-based classification at the system level. Version 5 covers assets including, but not limited to, servers, workstations, laptops, managed network switches, routers, firewalls, storage controllers, microprocessor relays, and generation control systems.

While CIP is identified as a separate risk element, discussed below in this report, it is important that the CIP standards themselves are also linked to other risk elements identified in this document. Staff that assess compliance to the CIP standards are encouraged to coordinate with Operations and Planning staff to ensure that the appropriate risks are identified and addressed.

Physical Security NERC Reliability Standard CIP-014-2

Background

On November 20, 2014, FERC approved CIP-014-2 – Physical Security, which NERC along with industry stakeholders developed in response to a March 7, 2014 FERC order directing the development of a standard that addresses physical security threats and vulnerabilities. The standard requires electric utilities to identify and protect transmission stations and transmission substations, as well as their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or cascading within an interconnection. CIP-014-2 became effective on October 1, 2015.

Risk-Based Approach to Compliance Monitoring and Enforcement

Risk-Based Compliance Monitoring

Risk-based compliance monitoring involves the use of the ERO Enterprise Risk-Based Compliance Oversight Framework (Framework). The Framework focuses on identifying, prioritizing, and addressing risks to the BPS, which enables each CEA to direct resources where they are most needed. REs are responsible for tailoring their monitoring (i.e., monitoring tools and the frequency and depth of monitoring engagements) of registered entities using the Framework, described in more detail within the Overview of the ERO Enterprise's Risk-based CMEP.

During 2017 and beyond, CEAs will continue deploying processes and tools to support risk-based compliance monitoring. NERC and the REs are committed to ensuring full transformation to risk-based compliance monitoring, and plan to continue communications, training, and outreach throughout 2017.

As reliability risk is not the same for all registered entities, the Framework examines BPS risk of registered entities both collectively and individually, to determine the most appropriate CMEP tool to use when monitoring a registered entity's compliance with NERC Reliability Standards. The Framework also promotes an examination into how registered entities operate and tailors compliance monitoring focus to areas that pose the greatest risk to BPS reliability. The Framework elements are dynamic and are not independent; rather, they are complementary and dependent on each other.

The IP contains the ERO Enterprise risk elements, which provide guidance to REs in the preparation of their RE IPs. REs are expected to consider regional risks and specific circumstances associated with individual registered entities within their footprints when developing compliance oversight plans. The process for identifying ERO Enterprise and RE risk elements, and their associated areas of focus, is explained later in the document.

The REs determines the type and frequency of the compliance monitoring tools (e.g., offsite or onsite audits, spot checks, or self-certifications) that are warranted for a registered entity based on reliability risks. The Inherent Risk Assessment (IRA) involves a review of potential risks posed by an individual registered entity to the reliability of the BPS.[3] An IRA considers factors such as assets, systems, geography, interconnectivity, and overall unique entity composition. In considering such factors, an IRA is not limited by the risk elements and associated areas of focus identified in the 2017 ERO Enterprise CMEP IP. Rather, the IRA considers multiple factors to focus oversight to entity-specific risk and results in the identification of the standards and requirements that should be monitored.

When developing more-specific monitoring plans for registered entities in their footprints, the REs also take into account prior compliance history, mitigating activities associated with prior noncompliance, and any information obtained through the processes outlined in the Internal Control Evaluation (ICE) Guide.[4] As a result of the ICE, and other considerations, the REs may further reduce the focus of compliance monitoring activities for a given entity, and may, for example, limit the depth and testing for a given area.[5]

[3] ERO Enterprise Inherent Risk Assessment Guide, available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Inherent_Risk_Assessment_Guide_20141010.pdf

[4] ERO Enterprise Internal Control Evaluation Guide, available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Internal%20Control%20Evaluation%20Guide.pdf

[5] For example, if a registered entity demonstrates effective internal controls for a given Reliability Standard during the ICE, the RE may determine that it does not need to audit the registered entity's compliance with that Reliability Standard as frequently, or the RE may select a different monitoring tool.

Coordinated Oversight of Multi-Region Registered Entities

The ERO Enterprise offers a coordinated oversight program of multi-region registered entities (MRREs).[6] The Coordinated Oversight Program for MRREs is designed to streamline risk assessment, compliance monitoring and enforcement, and event analysis activities for the registered entities that use, own, or operate assets in areas covering more than one RE territory.

Under the Coordinated Oversight Program for MRREs, REs will coordinate their oversight responsibilities over MRREs by designating one Lead RE (LRE) to each MRRE or a group of MRREs.[7] The LRE is selected based on BPS reliability considerations and the registered entity's operational characteristics. The selected LRE works collaboratively with the remaining Affected REs, known as AREs, and informs NERC of activities as appropriate. The Coordinated Oversight Program is flexible and voluntary for MRREs.

Compliance Assessments for Events and Disturbances

An important component of the ERO Enterprise's risk-based approach to compliance monitoring is voluntary participation in the Compliance Assessment (CA) Process by registered entities after an event or disturbance. Through the Event Analysis Process, the ERO Enterprise promotes a culture of reliability and security excellence that encourages an aggressive and critical self-review and analysis of operations, planning, and critical infrastructure performance.

The CA Process is a complementary review of the event focused on the evaluation of compliance with Reliability Standards. A registered entity completes a CA by reviewing the facts and circumstances of an event or disturbance, identifying relevant Reliability Standards and Requirements, evaluating compliance with these standards and requirements, and self-reporting any potential noncompliance. RE compliance staff also assess significant events and disturbances to increase awareness of reliability risks that may guide further compliance monitoring activities.

Registered Entity Responsibilities in CA Process

The ERO Enterprise encourages registered entities to perform a voluntary, systematic CA in response to all system events and disturbances. Registered entities are also encouraged to share the CA with the RE for all Category 2 and above events. Registered entities should use the Sample Compliance Assessment Report template (Appendix B of this document) when performing a CA. In addition to the completed CA template, registered entities should provide to the RE sufficient event information, such as the Brief Report or Event Analysis Report, so the RE may thoroughly understand the event.

Registered entities that follow the process above to evaluate systematically their own compliance performance, self-report potential noncompliance, and address reliability issues demonstrate the effectiveness of their internal controls and their commitment to a culture of compliance. Registered entities that are able to demonstrate strong internal controls and a robust culture of compliance that mitigates risk may be afforded some recognition by way of reduced levels and frequency of compliance monitoring activities. Mitigating credit for these actions is also considered during the enforcement of a noncompliance. Such credit may be available to the registered entity for comprehensive CAs that clearly demonstrate a systematic review of applicable standards and, as appropriate, self-reporting.

[6] Coordinated Oversight of MRRE Program Development and Implementation, available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Coordinated%20Oversight%20MRRE%20_FAQ%20(002).pdf and Compliance Monitoring and Enforcement for Entities Registered in Multiple Regions Webinar – June 23, 2015, available at http://www.nerc.com/pa/comp/Pages/RAI-Workshops-and-Webinars.aspx.

[7] The intent of the Coordinated Oversight Program of MRREs is to have a single LRE. However, although not anticipated, if needed there may be multiple LREs.

Regional Entity Responsibilities in CA Process

REs will review system event reports and CA reports provided by registered entities and may use a risk-based approach to prioritize these evaluations. However, the REs will conduct a Regional Compliance Evaluation (RCE) for all Category 2 and above events. The RE may also examine lower category events that indicate the need for closer examination. As part of its independent evaluation of the CA, the RE may request additional information from the registered entity if it is needed to better understand the event. This process, while informal, may be used to recommend a formal compliance monitoring method, such as a spot check, or be used to recommend a modification to the scope of an upcoming audit.

The scope of RCEs and the manner in which the REs and NERC evaluate, process, and respond to these reviews should reflect the significance of the event. The registered entities can greatly assist the REs by providing thorough and systematic self-evaluations in their CAs. The RE will share the RCE and CA with NERC staff.

Risk-Based Enforcement

The ERO Enterprise's risk-based enforcement defines, communicates, and promotes desired entity behavior in an effort to improve the reliability of the BPS. Specifically, risk-based enforcement allows the ERO Enterprise to focus on higher risks to the reliability of the BPS while maintaining the ERO Enterprise's visibility into potential noncompliance, regardless of the level of risk they pose. NERC has transitioned its oversight activities to align with the risk-based CMEP, which has allowed the ERO Enterprise to focus on issues that pose greater risk to reliability. NERC staff conducts qualitative reviews on a continuing basis on various aspects of the risk-based CMEP to evaluate the effectiveness of CMEP strategies and program execution. In addition, these reviews identify and incorporate best practices and guidance for REs.

Enforcement Philosophy

The ERO Enterprise continues to refine its risk-based enforcement philosophy. The ERO Enterprise's risk-based enforcement philosophy generally advocates reserving formal enforcement actions for those issues that pose a higher risk to the reliability of the BPS. The risk of a noncompliance is determined based on individual facts and circumstances, including any compensating or mitigating factors that existed during the pendency of the noncompliance. The ERO Enterprise works with registered entities to ensure timely remediation of potential risks to the reliability of the BPS and to prevent recurrence of the noncompliance. The enforcement process allows parties to address risks collaboratively and promote increased compliance and reliability through improvement of programs and controls at the registered entities.

For issues posing a minimal risk to the BPS, NERC and the REs may exercise appropriate judgment whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes as Compliance Exceptions. The availability of streamlined treatment of minimal risk noncompliance intended to encourage prompt identification and correction of issues by registered entities and the efficient mitigation of such issues in the enforcement process. As such, while self-identified minimal risk noncompliance is more than likely not going to be subject to a financial penalty, registered entities are encouraged to establish robust internal controls to prevent, detect, and correct noncompliance. This approach allows the ERO Enterprise to oversee the activities of registered entities in a more efficient manner and to focus resources where they result in the greatest benefit to reliability.

An inherent element of a risk-based approach to enforcement is accountability of registered entities for their noncompliance. No matter the risk of the noncompliance, the registered entity still bears the responsibility of mitigating that noncompliance and working to prevent recurrence. Based on the risk, facts, and circumstances associated with that noncompliance, the RE decides on an appropriate disposition track, inside or outside of an enforcement action, as described above. The RE also determines whether a penalty or sanction is appropriate for the noncompliance.

Penalties and sanctions are generally warranted for some moderate risk violations and most, if not all serious risk violations (e.g., loss of load, CIP program failures). Penalties and sanctions are also frequently assessed when repeated noncompliance of the same or similar Reliability Standard constitutes an aggravating factor. In addition to the use of significant penalties to deter undesired behavior, the ERO Enterprise also incents desired behaviors. Specifically, REs may offset penalties to encourage valued behavior. Factors that may mitigate penalty amounts for valued behavior include registered entity cooperation, accountability (including acceptance of responsibility for violations), culture of compliance, and self-identification of noncompliance.

REs may also grant credit in enforcement determinations for certain actions undertaken by registered entities for improvements that increase reliability and/or security. For example, REs may consider significant investments in tools, equipment, systems, or training made by registered entities, beyond those typically used in the industry or otherwise planned or required for compliance or mitigation, as an offset for proposed penalties in enforcement determinations. REs do not award credits or offsets for actions or investments undertaken by a registered entity that are required to mitigate the noncompliance or meet the requirements of future Reliability Standards.

Compliance Exceptions Annual Review

The use of Compliance Exceptions[8] continues to allow the ERO Enterprise to dispose of noncompliance posing a minimal risk to the reliability of the BPS efficiently, and enhance its focus on noncompliance posing a greater risk to BPS reliability. In June 2016, NERC and FERC completed their first annual review of Compliance Exceptions in combination with the annual Find, Fix, Track, and Report sampling. Notably, FERC and NERC staff agreed with the final risk determinations for all samples and observed significant improvement in the clear identification of root cause. NERC anticipates the next Compliance Exception annual review, beginning in October 2016, will likewise show continued improvement and consistency in RE use of Compliance Exceptions.

Self-Logging Program Process Review

Through the Self-Logging program, the ERO Enterprise encourages registered entities to detect, accurately assess, and correct minimal-risk noncompliance with Reliability Standards. In July 2016, NERC began a Self-Logging Process Review to evaluate the consistency of each REs practices and to ensure compliance with the NERC CMEP and the Self-Logging program document.[9] The purpose of this effort was to capture a snapshot, across all eight REs, of the processes for self-logging. Using the results of this review, the ERO Enterprise is considering any barriers to increased levels of participation in the program and identifying best practices by those REs that have accomplished broad industry participation in self-logging. The ERO Enterprise will then use this information to enhance the program and encourage greater involvement from registered entities.

[8] Compliance Exception Overview available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf

[9] ERO Enterprise Self-Logging program available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Updated_ERO%20Enterprise%20Self-Logging%20Program%20(2-1-16).pdf

Risk-Based Compliance Oversight Plan

Process for Risk Elements and Associated Areas of Focus

As noted above, the ERO Enterprise utilizes the Framework to identify risks to the reliability of the BPS, as well as mitigating factors that may reduce or eliminate a given reliability risk. As such, NERC identifies risk elements using data including, but not limited to: compliance findings; event analysis experience; data analysis; and the expert judgment of NERC and RE staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee). NERC uses these risk elements to identify and prioritize interconnection and continent-wide risks to the reliability of the BPS. These identified risks, as well as risks to the reliability of the BPS identified by each RE for its footprint, will be used by REs to focus monitoring activities, and will be used as inputs for developing oversight plans for individual registered entities.

For the purpose of the IP, areas of focus highlight ERO Enterprise-wide and RE-specific risks that merit increased focus for compliance monitoring, which may become a part of an individual registered entity's compliance oversight plan. The areas of focus do not represent the exclusive list of important or relevant Reliability Standards or Requirements, nor the entirety of the risks that may affect the reliability of the BPS. Rather, REs will consider the risk elements and areas of focus to help prioritize compliance monitoring efforts.

When developing entity-specific compliance oversight plans, REs consider local risks and specific circumstances associated with individual registered entities. The compliance oversight plan also takes into account the unique compliance history of each registered entity, along with both the timing of and the results of any prior compliance monitoring, when determining which compliance monitoring tools will be used for future monitoring for each registered entity. The compliance oversight plan focuses on a complete picture of reliability risks associated with a registered entity along with various mitigating factors, such as past performance or the presence of effective internal controls, to determine the appropriate compliance monitoring tool for registered entities.

As a result, a particular registered entity's scope of monitoring may include more, fewer, or different Reliability Standards than those outlined in the ERO and RE CMEP IPs. The determination of the appropriate CMEP tools may be adjusted, as needed, within a given implementation year. Additionally, NERC and the REs have the authority to monitor compliance with all applicable Reliability Standards whether they are identified as areas of focus to be considered for compliance oversight in the annual IP or are included in an RE's oversight plan for a registered entity.

NERC followed the risk element development process to review and reassess the 2016 risk elements to determine applicability for 2017.[10] Although the IP identifies NERC Standards and Requirements for consideration for focused compliance monitoring, the ERO Enterprise recognizes by using the Framework and risk-based processes that REs will develop a focused list of NERC Reliability Standards and Requirements specific to the risk a registered entity poses. Therefore, a particular area of focus under a risk element does not imply (1) that the identified NERC standard(s) fully addresses the particular risk associated with the risk element, (2) that the identified NERC standard(s) is only related to that specific risk element, or (3) that all requirements of a NERC standard apply to that risk element equally. Subject to NERC monitoring, REs will consider the ERO Enterprise risk elements, along with RE risk elements, when conducting compliance monitoring activities and assessing compliance with identified NERC standards and requirements.

[10] Risk Elements Guide for Development of the 2015 CMEP IP, available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf.

Risk Element Results

The 2017 risk elements are the same as the 2016 risk elements. Table 1 compares the 2015, 2016, and 2017 risk elements.

Table 1: Critical Comparison of 2015, 2016, and 2017 Risk Elements

2015 Risk Elements	2016 Risk Elements	2017 Risk Elements
Cyber security	Critical Infrastructure Protection	Critical Infrastructure Protection
Extreme Physical Events	Extreme Physical Events	Extreme Physical Events
Infrastructure Maintenance	Maintenance and Management of BPS Assets	Maintenance and Management of BPS Assets
Monitoring and Situational Awareness	Monitoring and Situational Awareness	Monitoring and Situational Awareness
Protection System Misoperations	Protection System Failures	Protection System Failures
Uncoordinated Protection Systems		
Long-Term Planning and System Analysis	Event Response/Recovery	Event Response/Recovery
	Planning and System Analysis	Planning and System Analysis
Human Error	Human Performance	Human Performance
Workforce Capability	(N/A for 2016)	(N/A for 2017)

2017 Risk Elements

The risk elements below are not a comprehensive list of all risks to the reliability of the BPS. Standards, requirements, and associated functions for each area of focus may be updated throughout the year to reflect new versions of the standards that become effective. Where issues are being addressed through other mechanisms, they are not included herein for compliance assurance activities.

NERC identified the risk elements listed below using the risk element development process which includes taking into account the risks noted in the ERO Top Priority Reliability Risks 2014 - 2017 as well as in the Reliability Issues Steering Committee's (RISC) yearly ERO Priorities: RISC Updated and Recommendation report. Area of focus are provided for each of the risk elements. The areas of focus do not represent the exclusive list of important or relevant Reliability Standards or Requirements, nor are the areas of focus the entirety of the risks that may affect the reliability of the BPS. Rather, REs will consider the risk elements and areas of focus to help prioritize compliance monitoring efforts. Standards identified as areas of focus that will become inactive during the course of 2017, have been identified along with the succeeding version of the standard, or area focus, in each of the corresponding risk element tables listed below.

Critical Infrastructure Protection

The protection of critical infrastructure remains an area of significant importance. The risk includes threats and vulnerabilities that result from (1) system downtime, (2) unauthorized access, and (3) corruption of operational data.

While CIP is identified as a separate risk element, the CIP standards themselves are also linked to other risk elements identified in this document. The CIP standards address protection of the Bulk Electric System (BES); thus, errors in identifying and categorizing the appropriate BES components could lead to ineffective or missing security measures. There are also situations in which Operations and Planning standards could affect CIP risk elements (e.g., CIP-008 and CIP-009 deal with response planning and recovery from cyber events and as such could have been included as part of the Events Response/Recovery risk element).

System Downtime

NERC has analyzed data and identified that outages of tools and monitoring systems are fairly common occurrences. Events involving a complete loss of SCADA control, or monitoring functionality for 30 minutes or more, are the most common grid-related events since 2012 and limit the situational awareness of operators.

Inadequate situational awareness has the potential for significant negative reliability consequences and is often a precursor event or contributor to events. Lack of situational awareness has played a significant role in previous large scale events. Additionally, insufficient communication and data regarding neighboring entities' operations could result in invalid assumptions of another system's behavior or system state.

Unauthorized Access

Unauthorized access can lead to Bulk Cyber Systems (BCSs) being compromised and is a major risk to systems that are used to monitor and control the BES. The RISC report describes the implementation of mandatory CIP standards and the establishment of the Electricity Information Sharing and Analysis Center (E-ISAC) as substantial risk mitigation measures, but cyber-attack is a constantly evolving threat. Any communication gaps between cyber experts and industry operators could lead to vulnerabilities. Also, the fast-paced rate of changes in technology with increased reliance on automation, remote control technology, and grid sensors that enable the close monitoring and operations of systems means that advanced tools are needed to counter those threats.

Corruption of Operational Data

Misconfiguration of BES Cyber Assets, which often results from gaps in change management processes, can make the devices used to monitor and control the BPS vulnerable to more attacks.

Areas of Focus

Table 2: Critical Infrastructure Protection

Standard	Requirements	Entities for Attention	Asset Types
CIP-002-5.1	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Back up Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-005-5	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-006-6	R1, R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations

Table 2: Critical Infrastructure Protection			
Standard	**Requirements**	**Entities for Attention**	**Asset Types**
CIP-007-6	R1, R2, R3, R5	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations

Extreme Physical Events

Extreme physical events can include extreme natural events or physical security vulnerabilities that cause extensive damage to equipment and systems. As concluded in the RISC report, the potential consequences of such events are high enough to warrant increased focus to properly address the risk.

Extreme Natural Events

The RISC report identifies severe weather events (e.g., hurricanes, tornadoes, polar vortices, Geomagnetic Disturbances, etc.,) as physical events that, at the extreme, can cause equipment damage that is interconnection-wide, lead to fuel limitations, and disrupt telecommunications. Because of the long lead time needed to manufacture and replace some BPS assets, an extreme natural event that causes extensive damage to equipment could result in degraded reliability for an extended period of time.

Physical Security Vulnerabilities

The second component of extreme physical events are physical security vulnerabilities. As stated in the RISC report, coordinated sabotage such as localized physical attacks of significance or electromagnetic pulse (EMP) attacks are physical events that, at the extreme, can cause extensive interconnection-wide equipment damage and disrupt telecommunications. As previously mentioned, the lead time for manufacturing and replacing some BPS assets could result in degraded reliability for an extended period of time.

Areas of Focus

Table 3: Extreme Physical Events			
Standard	**Requirements**	**Inactive/Enforcement Date *(if applicable)***	**Entities for Attention**
EOP-010-1	R1, R3	n/a	Reliability Coordinator Transmission Operator
CIP-014-2	R1, R2, R3	n/a	Transmission Owner

Maintenance and Management of BPS Assets

As the BPS ages, lack of infrastructure maintenance is a reliability risk that continues to grow. The RISC report identifies that the failure to maintain equipment is a reliability risk exacerbated when an entity either does not have replacement components available or cannot procure needed parts in a timely fashion. Deficiencies in maintenance strategies create additional pressure on sparing programs and the ability to replace aging infrastructure. Another risk, highlighted by NERC's 2010 Facility Ratings Alert to industry, involved the misalignment between the design and actual construction of BPS facilities.

Additionally, compliance data analysis shows that PRC-005 has the highest number of reported noncompliance and serious or moderate risk filings of any non-CIP Standard in the past four years.

Transmission outages related to inconsistent vegetation management pose an ongoing reliability risk to the BPS. The 2015 Vegetation Report published by NERC shows a slight increase in grow-in vegetation-related outages.[11] As a result, NERC has included vegetation management as an area of focus again in 2017. FAC-003-4 addresses the risk of transmission outages, and associated potential for cascading events, due to vegetation growth in the transmission right-of-way.

Areas of Focus

Table 4: Maintenance and Management of BPS Assets			
Standard	**Requirements**	**Inactive/Enforcement Date *(if applicable)***	**Entities for Attention**
FAC-008-3	R6	n/a	Generator Owners Transmission Owners
PRC-005-6	R3, R4, R5	n/a	Distribution Providers Generator Owners Transmission Owners
FAC-003-4	R1, R2, R6, R7	n/a	Generator Owners Transmission Owners

Monitoring and Situational Awareness

Without the right tools and data, operators may not make decisions that are appropriate to ensure reliability for the given state of the system. NERC's *ERO Top Priority Reliability Risks 2014-2017* notes that "stale" data and lack of analysis capabilities contributed to the blackout events in 2003 ("August 14, 2003 Blackout") and 2011 ("Arizona-Southern California Outages"). Certain essential functional capabilities must be in place with up-to-date information available for staff to use on a regular basis to make informed decisions.

An essential component of Monitoring and Situational Awareness is the availability of information when needed. Unexpected outages of tools, or planned outages without appropriate coordination or oversight, can leave operators without visibility to some or all of the systems they operate. While failure of a decision-support tool is rarely the cause of an event, such failures manifest as latent risks that further hinder the decision-making capabilities of the operator. One clear example is the August 14, 2003 Blackout. NERC analyzed data and identified that outages of tools and monitoring systems are fairly common occurrences.

Areas of Focus

Table 5: Monitoring and Situational Awareness			
Standard	**Requirements**	**Inactive/Enforcement Date *(if applicable)***	**Entities for Attention**
IRO-005-3.1a	R1, R2	03/31/2017	Reliability Coordinator
IRO-002-4*	R3, R4	04/01/2017	Reliability Coordinator
**Replaces IRO-005-3.1a per dates noted*			
TOP-006-2	R1, R2, R7	03/31/2017	Balancing Authority Reliability Coordinator Transmission Operator
TOP-001-3*	R10, R11	04/01/2017	Balancing Authority Transmission Operator
**Replaces TOP-006-2 per dates noted*			

[11] 2015 Vegetation-Related Transmission Outages

Protection System Failures

Protection systems are designed to remove equipment from service so the equipment will not be damaged when a fault occurs. Protection systems that trip unnecessarily can contribute significantly to the extent of an event. When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary. This can also occur with Special Protection Systems, Remedial Action Schemes, Underfrequency Load Shedding, and Undervoltage Load Shedding schemes. Such coordination errors occurred in the Arizona-Southern California Outages (see recommendation 19)[12] and the August 14, 2003 Blackout (see recommendation 21).[13]

Additionally, a protection system that does not trip or is slow to trip may lead to the damage of equipment (which may result in degraded reliability for an extended period of time), while a protection system that trips when it shouldn't can remove important elements of the power system from service at times when they are needed most. Unnecessary trips can even start cascading failures as each successive trip can cause another protection system to trip.

Linkage between Misoperations and Transmission-Related Qualified Events - NERC *2016 State of Reliability* report (p.169).

An analysis of misoperation data and events in the event analysis process (EAP) found that in 2015 there were 50 transmission-related system disturbances which resulted in a Qualified Event[14]. Of those 50 events, 34 events, or 68 percent, had associated misoperations. Of the 34 events, 33 of them, or 97 percent, experienced misoperations that significantly increased the severity of the event. There were four events where one or more misoperations and a substation equipment failure occurred in the same event. The relay ground function accounted for 11 misoperations in 2014 causing events that were analyzed in the EAP. This was reduced to six events in 2015.

Areas of Focus

Table 6: Protection System Failures

Standard	Requirements	Inactive/Enforcement Date *(if applicable)*	Entities for Attention
PRC-001-1.1(ii)	R3, R4, R5	n/a	Generator Operator Transmission Operator
PRC-004-4(i)	R1, R5	04/01/2017	Distribution Provider Generator Owner Transmission Owner
PRC-004-5(i)*	R1, R5	04/02/2017	Distribution Provider Generator Owner Transmission Owner
**Replaces PRC-004-4(i) per dates noted*			

Event Response / Recovery

When events occur, the safe and efficient restoration of transmission service to critical load in a timely manner is of utmost importance. The RISC identified the effect of poor event response and recovery is far reaching and not only causes safety-, operational-, or equipment-related risks during restoration activities, but also contributes to prolonged transmission outage durations, thereby increasing the duration of BPS unreliability.

[12] See Arizona-Southern California Outages on September 8, 2011.
[13] See Final Report on the August 14, 2003 Blackout.
[14] See DRAFT ERO Event Analysis Process Version 3.1

An additional risk to event response and recovery is the unavailability of generators. Extreme weather conditions, severe cold, heat, and drought create significant stress on maintaining overall BPS reliability and present unique challenges for electric system planners and operators. These conditions can significantly increase residential and commercial electricity demand and consumption, at the same time imposing adverse generation impacts and fuel availability issues. Extreme weather conditions can also vary the amount of wind and clouds (fuel for variable energy resources) that impact the expected amount of available renewable generation in some areas.

When combined, the heightened electricity demand, increased potential for failure of power plant components, limitations on fuel supply availability, and competing use of certain fuels can lead to increased risks of adverse reliability impacts, including simultaneous forced outages, de-ratings, and failures to start of multiple generating units. When these severe conditions are present over large geographic areas, the combined impacts on the fuel supply, power plant operations, generation unavailability, and heightened electricity demand can lead to severe reliability impacts.

These extreme conditions occur beyond the extent of planned stress conditions, anticipated severe operation conditions, or fuel supply availability expectations. Further, the conditions can lead to imprecise forecasts of residential and commercial electricity demand, which is the baseline for planning the BPS and operators determining the amount of electric generation needed during critical periods. When the combination of some, or all, of these conditions occurs during these extreme incidents, the end result can be operations under severe unanticipated scenarios or a shortage of generation, prompting operators to implement curtailments or shed load in local areas to maintain reliability in the overall grid.

Areas of Focus

Table 7: Event Response / Recovery

Standard	Requirements	Inactive/Enforcement Dates *(if applicable)*	Entities for Attention
EOP-001-2.1b	R1, R2, R3	03/31/2017	Balancing Authority Transmission Operator
EOP-011-1*	R1, R2	04/01/2017	Balancing Authority Transmission Operator
**Replaces EOP-001-2.1b per dates noted*			
TOP-007-0	R1, R2, R3, R4	03/31/2017	Reliability Coordinator Transmission Operator
TOP-001-3*	R12, R14	04/01/2017	Reliability Coordinator Transmission Operator
IRO-001-4*	R1	04/01/2017	Reliability Coordinator Transmission Operator
**Replaces TOP-007-0 per dates noted*			

Planning and System Analysis

Planning and system analysis encompasses several areas (such as increased use of demand-side management, integration of variable generation, changes in load and system behavior, smart grid, increased dependence on natural gas, fossil requirements and retrofit outage coordination, nuclear generation retirements and outages, and resource planning). Uncoordinated planning can lead to situations where generation or transmission resources, or information concerning those resources, may be inadequate to ensure firm demand is served. The importance of adequate planning activities is further highlighted as a changing resource mix, deployment of new technologies, etc., can increase the risk to reliability if not properly considered in local planning cases.

NERC's annual *Long-Term Reliability Assessment*[15] forms the basis of NERC's assessment of emerging reliability issues.

Areas of Focus

Table 8: Planning and System Analysis			
Standard	**Requirements**	**Inactive/Enforcement Date *(if applicable)***	**Entities for Attention**
EOP-002-3.1	R4	03/31/2017	Balancing Authority
TOP-002-4*	R4, R5	04/01/2017	Balancing Authority
**Replaces EOP-002-3.1 per dates noted*			
TPL-001-4	R1, R2, R3, R4	n/a	Planning Coordinator Transmission Planner
FAC-014-2	R1, R5	n/a	Reliability Coordinator Transmission Operator

Human Performance

Human performance remains a key focus for the ERO Enterprise. Poor human performance generally refers to situations in which a human being makes a decision that contributes to operational errors. Stronger management and organizational support greatly contribute to the reduction and prevention of operational errors. Included in this subset are communication errors that can pose a significant potential risk to BPS reliability.

Areas of Focus

Table 9: Human Performance			
Standard	**Requirements**	**Inactive/Enforcement Date *(if applicable)***	**Entities for Attention**
COM-002-4	R5	n/a	Reliability Coordinator Transmission Operator Balancing Authority
PER-005-2	R3, R4	n/a	Reliability Coordinator Transmission Operator Balancing Authority

Regional Risk Assessments

When considering risk elements, REs will perform a Regional Risk Assessment to identify risks specific to their Region and footprint that could potentially impact the reliability of the BPS. After determining Region-specific risks, REs will also identify the related NERC Reliability Standards and Requirements associated with those risks to focus monitoring activities. The standards and requirements identified for RE risk elements are not intended to be a static list that must be examined during all compliance monitoring activities (e.g., scoping for a Compliance Audit). Rather, the risk elements identified by the RE will serve as input when conducting an IRA for a registered entity and ultimately in determining the scope of the entity's compliance oversight plan.

In the process of reviewing ERO risk elements to compile Regional Risk Assessments, REs are expected to:

- Gather and review RE-specific risk reports and operational information (e.g., interconnection points and critical paths, system geography, seasonal/ambient conditions, etc.);

[15] http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2014LTRA_ERRATA.pdf.

- Review and categorize potential RE-specific risks; and
- Identify associated Reliability Standards and Requirements for IRAs, ICEs, and ultimately the compliance oversight plan.

The RE IPs will describe the Region-specific risks that result from the Regional Risk Assessment. The RE IPs should explain how REs identified risks that affect their footprints, including the reasons any ERO risk elements identified above are not included or applicable to the RE footprint. Although each RE will consider risk elements, and may use similar risk considerations, the output of the Regional Risk Assessments may differ as a result of RE characteristics and the uniqueness of each RE's footprint. REs are encouraged to align their RE risk elements with the ERO risk elements as much as possible as RE risk elements should be viewed as incremental to the ERO risk elements.

Regional Compliance Monitoring Plan

Based on RE consideration and assessment of risk elements (ERO and/or Regional) and Regional Risk Assessments, each RE will develop a compliance monitoring plan, which in 2017 will include, at a minimum, the list of planned audits for Reliability Coordinators, Balancing Authorities, and Transmission Operators that are required to be performed at least once every three years, per the ROP. REs may also identify other registered entities that they will monitor through appropriate CMEP tools based on risk elements, Regional Risk Assessments, and the application of IRAs and ICEs.

2017 ERO Enterprise CIP Version 5 and CIP-014 Monitoring Approach

For 2017, the ERO Enterprise will continue a focused approach to monitoring compliance with CIP Version 5 and CIP-014-2. The goals of the 2017 monitoring approach include understanding program effectiveness supporting CIP Version 5 transition and CIP-014-2 implementation by identifying successes and challenges along with tailoring monitoring to appropriate risks. [16]

CIP Version 5

On July 1, 2016, the high and medium impact requirements for CIP Version 5 went into effect. Entity IRA and Compliance Monitoring Plans have helped to identify key risk for a given entity, however the ERO Enterprise will continue to focus on certain elements of cyber security for higher risk entities. The 2017 priorities will continue to address the Areas of Focus (as described on page 10) that were introduced in 2016. The priorities are further described below:

Generation facilities greater than 1500 MW - Based on the 2016 self-certification results, there are numerous generation facilities that, if compromised, could lead to grid instability. In addition, the technological complexity of these facilities' Distributed Control System (DCS), controllers and other BES Cyber Assets will require an analysis to determine if the risk of compromise is mitigated through the effective implementation of the standards.

Medium Impact BES Cyber Assets at Substations – Based on the self-certification results, the number of substations that contain cyber assets impacted by CIP has increased because CIP Version 5 no longer possesses the exclusion for non-Internet Protocol (non-routable) BES Cyber Assets. Therefore, additional focus may need to be applied to substations for higher risk entities and their higher impact substations.

[16] In addition to the ERO Enterprise monitoring identified in this section, REs will conduct audits based on their 2017 audit schedules and consider the ERO Enterprise and Regional risk elements and areas of focus when conducting risk-based activities throughout the year. IRA results may identify Reliability Standards and Requirements, beyond those identified within the ERO Enterprise and Regional CMEP IPs, for inclusion in the registered entity's compliance oversight plan based on the risk the entity poses to the BES.

Network Architecture – The continued evolution of network technology, virtualization, and telecommunications carriers has required that compliance monitoring processes and approaches also evolve in order to effectively assess entities modernization. As a result, the ERO Enterprise has invested in tools to help improve the ability of its auditors and engineers to assess the control systems network architecture. In 2017, network security as described in CIP-005-6 will be a focus of compliance monitoring engagements.

Low Impact BES Cyber Assets – The first substantial effective date for low impact BES Cyber Assets is April 1, 2017, however monitoring of compliance with the core technical requirements for identifying and securing sites that possess Low Impact External Routable connectivity has been delayed until further notice because the CIP Standard Drafting Team is actively modifying the language for these requirements. Therefore, the focus on low impact BES Cyber Assets for 2017 will be minimal.

Physical Security

As part of oversight of Reliability Standard CIP-014-2, ERO Enterprise staff have begun engaging Registered Entities through a variety of outreach activities and coordinated site visits to discuss and understand their implementation of CIP-014-2. Based on initial observations, from both NERC and RE staff feedback, industry is making progress towards effective implementation of and compliance with CIP-014-2.

The means and methods the ERO Enterprise will use to monitor compliance with the standard will emphasize assessing and supporting effective implementation.[17] The focus in 2015 and 2016 related to CIP-014-2's requirements to identify critical stations and substations, and that such identifications are appropriate and risk-informed. Working with system analysis subject matter experts in the ERO Enterprise, the 2017 focus will begin to address the following:

- Understanding and validating the scope of facilities identified as critical under CIP-014-2;
- The scope of security plans (i.e., the types of security and resiliency measures contemplated under the various security plans);
- The timeliness included in the security plans for implementing the security and resiliency measures; and
- Industry's progress in implementing the Reliability Standard.

Oversight of CIP-014-2 will also involve direct oversight of the Responsible Entities' CIP programs by NERC and, in some cases, with staff from Applicable Governmental Authorities (AGA). For example, FERC staff and NERC staff have been coordinating in support of joint visits of registered entities in 2016. While specific entities and scope of activities have not been fully determined, NERC anticipates continued coordination with FERC staff to minimize any duplication of effort, with emphasis given to ensure that Responsible Entity resources are not unnecessarily impacted.

NERC will continue providing regular communications and outreach to support industry's implementation of the standard. NERC and the REs have conducted webinars to reflect the most recent guidance communication throughout 2017, and it will continue providing updates via webinar and other means at key milestones during the implementation period. Going forward, NERC may also conduct additional workshops based on feedback from industry and in conjunction with Regional Entity outreach activities. Industry can access several NERC and RE outreach presentations on CIP-014-2.

[17] Prior guidance from February 9, 2015 related to the risk assessment and third party verifications required by the Reliability Standard also emphasized that compliance assurance activities will expect registered entities to be able to demonstrate that they implemented the requirement effectively. That guidance is available at: http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Memo%20to%20the%20ERO%20021015.pdf.

NERC Oversight of RE Compliance Monitoring

NERC collects and reviews the RE IPs prior to posting the final version of the ERO CMEP Implementation Plan. NERC oversight of the RE IPs will focus on how the REs conducted Regional Risk Assessments and how the assessments' results serve as an input into the overall compliance monitoring plans for registered entities.

While REs should document all processes, conclusions, and results used to develop registered entities oversight plans, they will not need to obtain prior approval from NERC on oversight plans. However, REs should maintain supporting documentation to supplement NERC's review.

The application of the Framework by the REs will reflect RE-specific circumstances including, as noted above, varying stages of conducting IRAs and ICEs. NERC oversight and regular training will ensure that all processes discussed herein are implemented in a consistent manner throughout the ERO Enterprise.

Appendix A1: Florida Reliability Coordinating Council (FRCC) 2017 CMEP Implementation Plan

This Appendix contains the Compliance Monitoring Enforcement Program (CMEP) Implementation Plan (IP) for the FRCC as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure.

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- FRCC has implemented a combined review process for entity non-compliance activities. The process will include subject matter experts from FRCC Monitoring, Risk, and Enforcement. This approach provides a streamlined process going into determination. The determination team will then provide a feedback loop to Monitoring and Risk for future Monitoring considerations and risk analysis of the entity.
- FRCC will continue to participate in Coordinated Oversight of entities that are registered in multiple regions (MRREs). Currently, three FRCC registered entities are participating in coordinated oversight. FRCC is an Affected Regional Entity (ARE) for each.
- FRCC will begin to implement processes and approaches related to the updated Inherent Risk Assessment (IRA) guide; ERO Enterprise Guide for Risk-based Compliance Monitoring.
- FRCC will continue its Critical Infrastructure Protection (CIP) Low Impact Outreach as identified in the Compliance Outreach section below.
- FRCC will review internal controls during an entity monitoring engagement to understand an entity's systems for measuring, reporting, and monitoring of their compliance program performance.

Other Regional Key Initiatives and Activities

- FRCC enforcement staff will continue to utilize the risk based enforcement methods. This includes the use of Compliance Exceptions as an option for disposition of minimal risk non-compliances and the use of Find, Fix, Track (FFT) as an option for minimal and moderate risk non-compliances.
- FRCC will continue to evaluate registered entities for potential inclusion into the Entity Self-Logging program, which allows those registered entities that have demonstrated effective management practices to keep track of minimal risk non-compliances (and associated mitigation) on a log that is periodically reviewed by FRCC.
- For those registered entities scheduled for an audit in 2017, FRCC will re-evaluate the existing initial IRAs and Compliance Oversight Plans (COP) prepared in 2016. The re-evaluation will be based on the review of Risk Elements identified in the 2017 Implementation Plan, and the 18 base Risk Factors.
- An Internal Control Evaluation (ICE) may be performed at the request of a registered entity to provide reasonable assurance and understanding of the entity's controls.

Regional Risk Assessment Process

The FRCC has reviewed the eight Electric Reliability Organization (ERO) identified Risk Elements and associated Areas of Focus and concurs with the specified Standards/Requirements in all the Areas of Focus with the following additions documented below in the Regional Risks and Associated Reliability Standards section.

FRCC will continue its annual process of receiving input from registered entity subject matter experts for FRCC compliance staff consideration on areas that they believe may contribute additional risk to the FRCC region. The input was received in May of 2016, which was also considered as part of our risk assessment process in developing our 2017 FRCC CMEP Implementation Plan.

FRCC considered the following local risk factors and identified additional Standards/Requirements for monitoring as detailed below in the Regional Risks and Associated Reliability Standards section.

Number and type of registered functions

As of September 28, 2016, FRCC has forty-seven (47) registered entities. The registered functions are further defined below:

- Balancing Authority
- Distribution Provider
- Generator Operator
- Generator Owner
- Planning Authority
- Resource Planner
- Reserve Sharing Group
- Transmission Operator
- Transmission Owner
- Transmission Planner
- Transmission Service Provider

The FRCC (Member Services division) is registered as a Reliability Coordinator (RC) and Planning Coordinator (PC). The SERC Regional Entity is the Compliance Enforcement Authority for these FRCC registered functions.

The FRCC has not identified any region-specific risks associated specifically with the number and type of registered functions within the FRCC, and therefore has not included additional Reliability Standards due to registered functions.

Geographic location, seasonal / ambient conditions, terrain and acts of nature

The area of the State of Florida that is within the FRCC Region is peninsular Florida east of the Apalachicola River. Areas west of the Apalachicola River are within the SERC Region. The entire FRCC Region is within the Eastern Interconnection and is under the direction of the FRCC RC.

The FRCC considers factors such as its susceptibility to tropical storms and hurricanes when considering additional Reliability Standards for inclusion in its monitoring activities. Such storms increase the probability of the region experiencing transmission line vegetation contact, significant imbalances in generation and load, the need to evacuate control centers, and the need to implement restoration plans. As a result, requirements of the Reliability

Standards for System Restoration from Blackstart Resources, Loss of Control Center Functionality, Transmission Vegetation Management, and Automatic Underfrequency Load Shedding have been added.

BPS transmission lines (circuit miles, voltage levels, IROL flowgates)

The FRCC has not identified any region specific risks associated with the bulk power system (BPS) transmission lines located in the FRCC region, and therefore has not included additional Reliability Standards due to BPS transmission line concerns.

BPS generation facilities

The FRCC has not identified any region specific risks associated with the BPS generation facilities located in the FRCC region, and therefore has not included additional Reliability Standards due to BPS generation facility concerns.

Blackstart Resources

Requirements of the Reliability Standard for System Restoration from Blackstart Resources are already included in the geographic location section above.

Interconnection points and critical paths

The FRCC region only connects to the Eastern Interconnection on the north side of the region due to its peninsular geography. Therefore, the FRCC considers factors such as susceptibility to system separation when selecting additional Reliability Standards for inclusion in its monitoring activities. As a result of the FRCC's limited interconnection points, and as also mentioned for geographic location previously, requirements of the Reliability Standard for Automatic Underfrequency Load Shedding have been added.

Special Protection Schemes (SPS)

The FRCC considers factors such as any major SPS installed in the FRCC region when considering additional Reliability Standards for inclusion in its monitoring activities. As a result of a major SPS in the FRCC region, and as also mentioned for geographic location and interconnection points previously, requirements of the Reliability Standards for Automatic Underfrequency Load Shedding, Special Protection System Misoperations, and Special Protection System Maintenance and Testing have been added.

System events and trends

The FRCC considers system events within the FRCC region when considering additional Reliability Standards for inclusion in its monitoring activities. External events are reviewed and considered in NERC's Risk Elements. As no major internal events have occurred recently, FRCC has not included additional Reliability Standards due to system events and trends.

Compliance history trends

The FRCC considers historical compliance trends within the region when considering additional Reliability Standards for inclusion in its monitoring activities. No significant compliance trends have been identified in the FRCC Region to justify the addition of any Reliability Standards.

Regional Risk Elements and Areas of Focus

The table below contains the Regional risk focus areas identified during the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of the registered entities compliance oversight plan.

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard(s) and Requirement(s)**
Extreme Physical Events	The FRCC's peninsular geography along with its susceptibility to hurricanes and limited connections to the Eastern Interconnect increases the risk of an event occurring resulting in system restoration from Blackstart Resources.	EOP-005-2 R10
Extreme Physical Events	FRCC's susceptibility to hurricanes increases the risk of a control center becoming inoperable.	EOP-008-1 R6
Maintenance and Management of BPS Assets	Lack of access to the transmission system, along with environmental regulations make accessing the transmission corridors difficult for maintenance crews.	FAC-003-4 R5
Extreme Physical Events	The FRCC's peninsular geography along with its susceptibility to hurricanes, and limited connections to the Eastern Interconnect increases the dependency on proper UFLS program implementation. Also, the region has a significant RAS that could result in islanding and UFLS activation.	PRC-006-2 R9
Extreme Physical Events and Protection System Failures	The FRCC region has RAS separation schemes that could impact a major portion of the FRCC if they do not operate as planned.	PRC-016-1 R1 & R2 PRC-017-1 R1

Regional Compliance Monitoring Plan

By the end of 2016, FRCC will have completed initial IRAs for all registered entities in the region. In 2017 FRCC will evaluate the need to re-perform an IRA for each registered entity scheduled for an audit, a spot check, or a self-certification under any update approaches from the implemented updated IRA guide as mentioned above in section one. For all other registered entities an IRA may be updated at any time.

The following list includes potential triggers that may initiate a partial or complete IRA update.

- Three years since the last update;
- 210 days prior to a scheduled Compliance Audit;
- Applicable additions or reductions to the ERO or FRCC identified Risk Elements;
- Functional Registration changes of the registered entity;
- Events/disturbances/exceedances/mis-operations associated with, or significant to, a registered entity;
- Compliance history review (Self-Certifications, Violations, Mitigations, etc.) of a registered entity;
- Significant changes to the registered entity's asset (Transmission, Generation, Distribution, SCADA/EMS, CIP, etc.) portfolio(s);

- Significant changes in the registered entity's organizational structure; or
- Any other changes to a registered entity's risk profile identified by FRCC Compliance staff.

Periodic Data Submittals

FRCC has identified the Reliability Standards and requirements listed in the table below that require Periodic Data Submittals. The Quarterly data submittals are due by the 15th of the month following the previous quarter. All data submittals are to be submitted via the Compliance Tracking and Submittal system (CTS).

For Quarterly submittals for FAC-003-4 R1 and R2, if an entity does not have any Sustained Outage(s) during a respective quarter, they are not expected to submit a quarterly report. In turn, FRCC will advise NERC that there were no Sustained Outages within the quarter. However, entities are expected to submit a FAC-003-4 Event form for ALL Sustained Outages within the quarter in which the event occurs, as specified in the standard. While not specifically required by FAC-003-4, FRCC strongly encourages and appreciates entities' reporting, within 48 hours, all Sustained Outages for Categories 1A&B, 2A&B and 4A&B utilizing the FAC-003-4 Event form. FRCC will be notified when an event is reported by the CTS system and will follow-up accordingly with the submitting entity and NERC.

2017 Periodic Data Submittal Plan	
Standard & Requirement	**Justification**
FAC-003-4 R1, R2	Sustained Outage data submitted quarterly by applicable registered entities

Self-Certifications

For 2017 compliance monitoring, FRCC will continue to utilize the Self-Certification process with a risk based approach. FRCC will use Self-Certification in a coordinated approach with the other compliance monitoring methods. This will address the Standards and requirements that represent the greatest risk to the reliability to the Bulk Power System (BPS) based on the results of the registered entities' overall Inherent Risk Assessments (IRA) and the addition of new Standards/Requirements that become enforceable during the 2017 year. FRCC will utilize Self-Certification for registered entities to Self-Certify compliance with those Standards and Requirements identified through the IRA process.

The registered entity will provide FRCC with the methodology and other supporting documentation used for self-assessment to determine the compliance status for those requirements. This approach will include more information on the expectations of what the registered entity should consider and include in their response to the FRCC. FRCC will verify the accuracy of the Self-Certification determinations and, if further substantiation is needed, FRCC may conduct a Spot Check of the work or include the applicable Standards and Requirements in a future Compliance Audit.

Spot Checks

FRCC will conduct Spot Checks on all applicable registered entities for the CIP-014-2 R1, R2. FRCC reserves the right to initiate random spot checks in response to operating problems or concerns.

Compliance Audits

The table below identifies the registered entities scheduled for an On-Site Audit in 2017 and is based on the individual registered entities' IRAs.

2017 Compliance Audit Plan			
NCR #	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR00037	Homestead, City of	O&P	
NCR00074	Tampa Electric Company	O&P	CIP
NCR00040	JEA	O&P	CIP
NCR00032	Gainesville Regional Utilities	O&P	

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	Anticipated Date
Spring Compliance Workshop (FRCC Combined O&P and CIP)	April 11-12, 2017
Fall Compliance Workshop (FRCC Combined O&P and CIP)	November 7-8, 2017
Reliability Standard Webinars	Periodic
Additional Compliance Workshop (as needed)	TBD
CIP V5 Low Impact Outreach	TBD

Appendix A2: Midwest Reliability Organization (MRO) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the MRO as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

For 2017 oversight monitoring MRO began developing Compliance Oversight Plans (COPs) for registered entities within its footprint. The goal of this effort is to provide multi-year COPs for each registered entity that contain planned oversight scope, monitoring intervals, and monitoring methods.

MRO updated its internal Inherent Risk Assessment (IRA) process to align with the revised 2017 Electric Reliability Organization (ERO) Compliance Monitoring Enforcement Program (CMEP) IP and Risk Elements.

Other Regional Key Initiatives & Activities

Mitigating Activities for Compliance Exceptions

As part of the Annual Implementation Plan, MRO staff will periodically sample Compliance Exceptions, including those submitted through Self-Logging, to verify that the mitigating activities have been completed. The sample will come from only those Compliance Exceptions that have been identified by a registered entity as already mitigated or Compliance Exceptions that have a planned mitigation date that has passed. Also, the Compliance Exceptions sampled are not restricted to the registered entities that have an IRA performed on them for 2017.

Periodic sampling may occur at any time within 18 months from the later of the date of issuance of a Notice of Compliance Exception Treatment or the date the registered entity completed mitigation activities, and will be reviewed through informal means, Spot Checks, or during a normally scheduled Compliance Audit. MRO staff are required to document the results regardless of whether a formal or informal review process is used.

All mitigation activities relating to enforcement matters that are filed with regulators will be verified for completion.

Regional Risk Assessment Process

MRO's Regional Risk Assessment (RRA) process consists of a broad assessment of all known risks at the regional level. The MRO RRA involves a comprehensive review of regional data and trends, geography and topology, events, violations, high risk Standards and Requirements, and other regionally identified risks. The 2017 MRO RRA did not identify any unique regional Risk Elements to add to the suite of ERO Risk Elements. In order to facilitate the analysis of standards and ensure that significant risks identified by both the MRO RRA and the ERO Risk Elements are addressed, MRO has organized requirements into Performance Areas. Evaluating Performance Areas helps to simplify the identification of those requirements that should be monitored in order to effectively address the risks that are known to exist.

A list of the 2017 MRO Performance Areas, described above, is available on MRO's website[18]. The posted document includes the name of each Performance Area along with a description of the associated risks and a list of requirements that address those risks.

[18] 2017 MRO Performance Areas

Regional Risk Elements and Areas of Focus

MRO did not identify any regional Risk Elements for 2017.

Regional Compliance Monitoring Plan

This section includes regional risk-based CMEP activities. Following is an overview of the year's currently known Inherent Risk Assessments (IRAs), Compliance Audits, Spot Checks, Periodic Data Submittals, and Self-Certifications.

Inherent Risk Assessments

The requirements that are associated with Performance Areas form the input to the IRA process for each entity. Risk factors, in addition to a detailed qualitative analysis of the entity, are used to quantify an entity's inherent risks and determine which requirements should be monitored for that entity. The final result of the IRA process is an entity-specific risk level for each requirement based on the entity's unique characteristics.

MRO plans to have completed an initial IRA for each registered entity within the region by the end of 2016. IRAs may be refreshed as determined by MRO on an as-needed basis for reasons such as, but not necessarily limited to, changes in registration, Bulk Power System (BPS) footprint, mergers, and acquisitions.

Compliance Oversight Plans

The IRA results for each registered entity will be used in conjunction with internal control information, compliance history, and other entity performance data to drive COP development. The COP contains the planned approach to compliance monitoring for a registered entity including standards/requirements to be monitored, the CMEP tool that will be used, and the interval of monitoring.

Compliance Audits

The following registered entities have been identified as being on the 2017 Compliance Audit schedule. Based on IRA results, additional registered entities may also be subject to a Compliance Audit in 2017.

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR01020 NCR05521 NCR01145	Xcel Energy (NSP, PSCO, SPS)	O&P	CIP
NCR00977	Corn Belt Power Cooperative	O&P	
NCR10192	ITC Midwest (RF Lead)	O&P	CIP
NCR01001	Lincoln Electric System	O&P	CIP
NCR00979	Dairyland Power Cooperative	O&P	CIP
NCR00824	MidAmerican Energy Corporation	O&P	CIP
NCR00992	Great River Energy	O&P	CIP

The audit schedule is also located on MRO's website here: MRO 2017 Audit Schedule

Spot Checks

There are no planned Spot Checks for 2017. However, if unique situations and/or unforeseen risks arise, Spot Checks may be used by MRO in 2017.

Periodic Data Submittals

The following requirements are scheduled to be subject to periodic data submittal monitoring in 2017.

Reliability Standards Subject to Periodic Data Submittals		
EOP-004-2 (Through 3/31/2017)	EOP-004-3 (Starting 4/1/2017)	FAC-003-4

Self-Certifications

For 2017, MRO will continue with the use of "guided" Self-Certifications, which focus more on risk and supporting evidence than the previous annual Self-Certifications. As part of the guided Self-Certification process, registered entities will provide MRO with supporting evidence to substantiate determinations.

These guided Self-Certifications are intended to provide MRO with reasonable assurance of compliance based upon the results of the registered entity's assessment. Where appropriate, MRO may utilize the guided Self-Certification instead of Compliance Audits or Spot Checks as the monitoring tool for specific Reliability Standards and Requirements. The guided Self-Certification process helps improve the effectiveness of oversight and increase efficiency by relying on the work of registered entities in meeting compliance requirements.

Part of the process of relying upon the work of others includes MRO performing a review of the work and evidence supporting the guided Self-Certification results. MRO may re-perform the work, in part, in order to verify the accuracy of the Self-Certification determinations. In the event that further substantiation is needed, MRO staff may conduct a random Spot Check of the work or include the applicable Standards and Requirements in a subsequent Compliance Audit. The overall goal of the guided Self-Certification process is to provide reasonable assurance that the entity meets compliance with the applicable Standards and Requirements.

Guided Self-Certifications will be performed over the implementation period (January 1 to December 31) on a quarterly basis for an identified baseline set of Reliability Standards that have been identified both through the Regional Risk Assessment process and an entity's IRA output. An entity will receive a Self-Certification for a specific requirement if output from that entity's IRA, and analysis performed within the entity's COP, identifies that requirement as being one that should be monitored through a Self-Certification. In other words, the input used by MRO to make this decision for each entity is based on a registered entity's specific inherent risk to the BPS and its compliance history.

The intent of the quarterly frequency is to disperse the workload, assuring sufficient time for completion and review, and to promote continuous self-monitoring of compliance.

2017 Guided Self-Certification Schedule		
Standard	**Requirement**	**Quarter**
FAC-008-3	R3	1
EOP-011-1	R1	2
CIP-003-6	R2	3
CIP-011-2	R1, R2	3
EOP-010-1	R3	4

Unless unique concerns are identified that MRO determines warrant a deeper look as part of a Compliance Audit, registered entities that receive a 2017 quarterly Self-Certification should not expect to get audited on the same requirement(s) in 2017.

In addition to the quarterly guided Self-Certification schedule, guided Self-Certifications may also be used for compliance monitoring as a result of IRAs, and for events that could or did negatively impact the reliable operation of the region or systems within the region.

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
MRO Newsletter	Six times a year
MRO Hot Topics	Periodically as needed
MRO Webinars	Periodically as needed
MRO Operations Conference	Summer 2017
MRO Security Conference	Fall 2017
MRO Compliance and Enforcement Conference	Fall 2017
Registered entity-specific conferences and meetings	Periodically as needed

Appendix A3 - Northeast Power Coordinating Council (NPCC) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the NPCC as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

NPCC will continue to support all Electric Reliability Organization (ERO) Enterprise committees, subcommittees, working groups, task forces, and other teams to improve risk assessment and controls evaluations that support compliance monitoring and enforcement activities within the ERO Enterprise.

NPCC has developed various regional specific tools to ensure that audits, spot checks, guided self-certifications, Inherent Risk Assessments (IRA), and Internal Control Evaluations (ICE) are performed in consistent fashion.

- Evidence tracking sheet (audits, spot checks)
- Guided Self-Certification worksheet
- Function specific IRA templates
- Matrix of NERC/NPCC Risk Elements that map to NERC Risk Factors
- Documented procedure and process flow diagrams for performing IRA and determining monitoring scope
- IRA Summary report
- ICE worksheet
- ICE summary report

A separate implementation plan will apply to entities registered in New Brunswick with the New Brunswick Energy and Utilities Board.

A separate implementation plan will apply to entities registered in Québec with the Régie de l'énergie.

Other Regional Key Initiatives and Activities

NPCC has instituted a program to perform CIP-014 gap analysis to assist the entities in fine-tuning their CIP-014 process. Results will be shared with the ERO.

NPCC has instituted a program to perform CIP V5 outreach for entities that have only Low impact facilities.

Regional Risk Assessment Process

NPCC coordinated with the other Regional Entities to develop the following 2017 ERO Risk Factors:

1. UFLS Equipment
2. UFLS Development and Coordination
3. UVLS
4. Load
5. Transmission Portfolio

6. Voltage Control
7. Largest Generator Facility
8. Variable Generation
9. Total Generation Capacity
10. Planned Facilities
11. CIP – Technical
12. ICCP - Connectivity
13. Critical Transmission
14. Balancing Authority Coordination
15. Remedial Action Schemes/Special Protection Systems
16. Workforce Capability
17. Situational Awareness and Monitoring Tools
18. System Restoration

In the development of the standards and requirements that appear in this regional plan, NPCC considered the 2017 ERO Risk Factors and other tangible Bulk Electric System (BES) attributes such as entity functional registration, transmission assets, Remedial Action Schemes, Blackstart plans and facilities, generation assets, role of Underfrequency Load Shedding (UFLS) , and historical events.

As a result, NPCC believes that the application of the Revised BES Definition may offer reliability exposure due to the over 1,000 newly captured BES elements within NPCC. The transmission portfolio of many entities has increased and several entities have increased operational responsibility associated with the newly captured elements. In 2016, the lone NPCC Regional Risk Element was termed "*Revised BES Definition*". Moving into 2017, it is more accurate to describe the Regional Risk Element as the "*Registration and Compliance Obligation Changes Associated with the BES Definition*". As a result, NPCC will place regional focus on standards and requirements associated with operations, maintenance, and planning for the following types of functional entities:

1. New TOPs, TOs, and TPs.
2. Existing TOs with an expanded pool of BES elements under their ownership umbrella.
3. Existing TPs with an expanded pool of BES elements under their planning umbrella.

Entities already registered as Reliability Coordinators (RCs), Balancing Authorities (BAs), or Transmission Operators (TOPs) do not fall under this Regional Risk Element.

In addition, NPCC recognizes the vital role that UFLS development and coordination play in minimizing and defending against a total system blackout. Due to this, NPCC has also added second Regional Risk Element called "*Coordination of UFLS Schemes*".

NPCC also expanded the requirements, with explanation, under several of the ERO Risk Elements.

NPCC has determined that none of the requirements included in the ERO Compliance Monitoring Enforcement Program (CMEP) Implementation Plan (IP) should be removed from the NPCC regional IP.

Regional Risk Elements and Areas of Focus

The table below contains the Regional risk focus areas identified during the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of the registered entities compliance oversight plan.

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Registration and Compliance Obligation Changes Associated with the BES Definition	On July 1, 2016, the effective date of the BES Definition resulted in new TOs, TOPs, and TPs being added to the NPCC registry. In addition, existing TOs, TOPs, and TPs were required to bring newly captured BES elements into their NERC compliance programs. Due to these factors, a significant number of BES elements became subject to the NERC Reliability Standards in NPCC for the first time. This situation, with such a substantial amount of elements undergoing a change related to NERC compliance obligations, is unique in the ERO to NPCC. NPCC will consider, on a functional basis, the requirements to the right for monitoring to assure that newly captured BES elements are included in important aspects of operations, maintenance, and planning. The functional types under focus are: 1. New TOPs, TOs, and TPs. 2. Existing TOs with an expanded pool of BES elements under their ownership umbrella. 3. Existing TPs with an expanded pool of BES elements under their planning umbrella. (Note: Requirements that are already captured as ERO Focus Areas are not included in the chart to the right. As a result, there are no requirements listed for existing TP's as TPL-001-4 is already an ERO Focus Area.)	**New TOPs** All of 2017 EOP-005-2 R1, R5, R6, R9, R10, R11, R12, R13 EOP-008-1 R1, R2, R4, R5, R6, R7, R8 FAC-014-2 R2 Until 3/31/17 EOP-001-2.1b R4, R5 IRO-004-2 R1 PER-001-0.2 R1 TOP-002-2.1b R1, R2, R4, R11, R17, R19 TOP-004-2 R1, R2, R3, R4, R5, R6 TOP-006-2 R3, R4, R5, R6 After 4/1/17 TOP-001-3 R1, R5, R6, R7, R8, R9, R13, R15, R16, R18, R19 TOP-002-4 R1, R2, R3, R6, R7 **New TOs** FAC-003-4 R3 FAC-008-3 R3 PRC-004-4i R4, R6 PRC-005-6 R1 **Existing TOs** FAC-003-4 R3 FAC-008-3 R3 PRC-004-4i R4, R6 **New TPs** FAC-014-2 R4

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Coordination of UFLS Schemes	Although rarely used, UFLS schemes are an extremely important aspect in limiting the extent of major disturbances. This is especially true in NPCC which has transmission corridors that are radial in effect. As such, NPCC recognizes that coordination in the design and implementation of UFLS programs are key in order to prevent a total system blackout like those that occurred in 1965, 1977, and 2003.	PRC-006-2 R3 (PC) R4 (PC) PRC-006-NPCC-1 R4 (TO, DP) R7 (TO, DP) R13 (GO)

Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Event Response/ Recovery	NPCC has identified differences in the implementation of manual load shed plans while conducting on-site audit interviews. NPCC will continue to monitor and discuss the entity's preparedness to shed load. Historical events in the Northeast (1965, 1977, 2003) have proven the need for thoroughly coordinated system restoration plans and activities, which includes training and simulation. The success of any system restoration cannot be accomplished without dependable blackstart resources that should be tested as per the TOP's process and have a procedure for energizing a bus. RC backup control centers with the functionality of the primary control center further ensures interconnection reliability and a more secure recovery from the loss of the primary.	EOP-003-2 (until 3/31/17) R1 (BA, TOP) R3 (BA, TOP) R5 (BA, TOP) R8 (BA, TOP) EOP-005-2 R1 (TOP) R9 (TOP) R10 (TOP) R13 (GOP) R14 (GOP) EOP-006-2 R1 (RC) R9 (RC) R10 (RC) EOP-008-1 R3 (RC)
Extreme Physical Events	The ability to mitigate the effects of geomagnetic disturbance (GMD) events is an expanded Risk Element within NPCC because Northern U.S. and Canadian terrain and latitudes offer more potential for a severe GMD event. In addition, past history also deems this to be an expanded risk element. A significant GMD event occurred on March 13, 1989 and resulted in a blackout of the power system in Quebec due to the tripping of shunt reactive devices. The dissemination of space weather information in R2 as per the GMD operating plan is vital to ensuring reliability.	EOP-010-1 (after 4/1/17) R2 (RC)

Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Monitoring and Situational Awareness	Historical events in the Northeast (1965, 1977, 2003) have proven the need for the highest level of RC/BA/TOP real-time operator monitoring capability, decision making, and situational awareness of current and near-term system status. To that end, the requirements listed will allow NPCC to confirm, educate, and discuss with the RC/BA/TOP as necessary on how the entity accomplishes the following: Ensuring proper reserves, taking action to alleviate BES risks, the degree that entities identify and operate to the most limiting parameter, issuing alerts and communicating without delay when foreseeing a transmission problem, performing next day analyses, performing 30 minute assessments, implementing real-time time plans to prevent SOL and IROL exceedences, and having documented data exchange policies that will ensure that it can perform real-time monitoring and assessments,	BAL-002-1 R1 (BA) R3 (BA) IRO-005-3.1a (until 3/31/17) R10 (RC, BA, TOP) R12 (RC) EOP-002-3.1a (until 3/31/17) R8 (RC) IRO-002-4 (after 4/1/17) R1 (RC) R2 (RC) IRO-008-1 (until 3/31/17) R1 (RC) R2 (RC) IRO-008-2 (after 4/1/17) R1 (RC) R2 (RC) R4 (RC) R5 (RC) IRO-009-2 R2 (RC) TOP-001-3 (after 4/1/17) R7 (TOP) R13 (TOP) R15 (TOP) R16 (TOP) R18 (TOP, BA) R19 (TOP) TOP-002-4 (after 4/1/17) R1 (TOP) R2 (TOP) R6 (TOP) TOP-004-2 (until 3/31/17) R1 (TOP) R2 (TOP)

Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Human Performance	Thoroughness of operator training in task performance and communication techniques will alleviate the risks of BES reliability events occurring in NPCC similar to those of 1965, 1977, and 2003. As such, NPCC wants to assure that entities verify/validate, at the highest levels, that entity personnel understand their role and the importance of following documented communication protocols during normal and emergency situations. NPCC also wants to ensure that entities training approach/methodology is in fact systematic, wants to garner an understanding of how entities are determining their list of specific BES reliability tasks, and wants to ensure that system restoration activity training is provided to field operators who may perform unique tasks.	COM-002-4 R1, R2, R4, R6, R7 (RC, BA, TOP) R3, R6 (GOP, DP) EOP-005-2 R11 (TO) PER-005-2 R1 (RC, BA, TOP) R2 (TO) R3 (TO)

Regional Compliance Monitoring Plan

This section includes regional risk-based CMEP activities. Following is an overview of the year's currently known IRA, ICE, audit, spot check, periodic data submittals, and guided self-certifications.

The 2017 NPCC Compliance Monitoring Plan is located here on the NPCC website.

Inherent Risk Assessment

Unless system events or the situation dictates otherwise, the 2017 NPCC Compliance Monitoring Plan will consist of those entities whose historical three-year cycle or historical six-year cycle occurs in 2017. NPCC will review the 2016 IRA that is on-file for those entities. NPCC will consider the 2017 ERO Risk Factors and update (if necessary) an entity's IRA which will then be used to determine the subsequent method/degree/scope of CMEP engagement for 2017.

The results of an IRA may shift the CMEP engagement of a registered entity from a 2017 off-site audit to a guided self-certification, a spot check, or some combination thereof. IRAs outside of the normal cycle can be triggered by a system event in the NPCC area, a NERC alert, results of a spot check, and/or results of a guided self-certification, or other trends and/or Areas of Concern resulting from NPCC monitoring or enforcement activities.

Internal Controls Evaluation

NPCC will offer to perform ICE on all registered entities having a 2017 onsite Operating and Planning (O&P) audit who wish to volunteer for it. The volunteering entity will receive the results in an ICE Summary Report prior to seeing the final scope in the Audit Notification Letter. Recommendations for alternative monitoring approaches from the ICE process will feed into the Spot Check and Guided Self Certification programs as noted below.

NPCC will also offer to perform ICE for those entities having offsite O&P audits in 2017 who wish to volunteer for it. Throughout 2017, NPCC will continue to provide upfront outreach and education to entities to promote participation in ICE.

NPCC does not plan to perform ICE in advance of Critical Infrastructure Protection (CIP) audits of entities whose compliance to Version 5 have not been baselined.

Audits

For both O&P and CIP, NPCC will continue to perform on-site audits of BAs, RCs and TOPs every three years and will use the IRA (and voluntary ICE) to scope the O&P audits. For all other functions, NPCC will perform internal reviews based on the six-year cycle using the IRA on file to determine the type of engagement and scope.

To assure that an entity has identified BES Cyber Assets properly, NPCC will perform a review of those entities that 1) have declared that they possess newly identified Medium Impact BES Cyber Assets and 2) had Critical Cyber Assets under CIP Version 3 that are now Low Impact under CIP Version 5.

Spot Check

On a case-by-case basis, NPCC may use a spot check that will be guided by the results of the IRAs in lieu of an audit.

Periodic Data Submittals

NPCC is not posting a schedule for Periodic Data Submittals for 2017. As such, any data requests will be implemented on an as-needed basis.

Guided Self Certifications

Each quarter, one or more Reliability Standards will be selected on a function basis for a guided Self-Certification. NPCC will use the Standards and Requirements identified in the 2016 ERO CMEP Implementation Plan and those identified in Section 3 of this document, and the results of IRA as the basis for selecting those that will be subject to a Guided Self-Certification.

Guided Self Certification Information

2017 Compliance Audit Plan On-Site			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR07160	New York Independent System Operator	O&P	
NCR07163	Niagara Mohawk Power Corporation	O&P	CIP
NCR07159	New England Power Company	O&P	CIP
NCR07184	Ontario IESO	O&P	CIP
NBCR001	New Brunswick Power Corporation	O&P	CIP
NCR07181	NYSEG	O&P	CIP
NCR07207	Rochester Gas and Electric	O&P	CIP
NCR07133	Long Island Power Authority	O&P	
NCR07228	Vermont Transco, LLC		CIP
NCR07180	NSTAR Electric Company		CIP
NCR07029	Central Maine Power Company		CIP
NCR07161	New York Power Authority		CIP

2017 Compliance Audit Plan Off-Site			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR00503	BNY Power Operations, LLC	O&P	
NCR10371	CCI Rensselaer LLC	O&P	
NCR10331	First Wind O&M, LLC	O&P	
NCR07102	Granite State Electric Company	O&P	
NCR07144	Millennium Power Partners, LP	O&P	
NCR07167	NAES Corporation - Lockport	O&P	
NIR	Quebec 1	O&P	
NCR07169	NAES Corporation - North Tonawanda	O&P	
NCR07161	New York Power Authority	O&P	
NCR07162	Niagara Generation, LLC	O&P	
NCR00126	North Attleborough Electric Department	O&P	
NCR07182	Ocean State Power	O&P	CIP
NIR	Quebec 2	O&P	
NCR10366	Noble Altona Windpark, LLC	O&P	
NCR10271	Noble Bliss Windpark, LLC	O&P	
NCR10367	Noble Chateaugay Windpark, LLC	O&P	
NCR10272	Noble Clinton Windpark, LLC	O&P	
NCR10273	Noble Ellenburg Windpark, LLC	O&P	
NCR10368	Noble Wethersfield Windpark, LLC	O&P	
NIR	Quebec 3	O&P	
NCR07187	Oswego Harbor Power LLC	O&P	
NCR07191	Peabody Municipal Light Plant	O&P	
NCR10369	Penobscot Energy Recovery Company	O&P	
NCR10342	Pinetree Power - Tamworth, Inc.	O&P	
NCR07195	Pittsfield Generating Company LP	O&P	
NCR10370	Power City Partners, LP	O&P	
NIR	Quebec 4	O&P	
NIR	Quebec 5	O&P	
NCR00130	Neptune Regional Transmission System LLC	O&P	
NCR11647	Brookfield Power US Asset Management LLC	O&P	
NCR11649	Third Taxing District of East Norwalk	O&P	
NCR11639	New York Transco LLC	O&P	
NCR11582	Evergreen Wind Power II, LLC	O&P	
NBCR	New Brunswick 1	O&P	
NBCR	New Brunswick 2	O&P	
NCR00543	TC Ravenswood LLC		CIP
NCR00893	PSEG Fossil LLC		CIP
NCR04057	Exelon Generation Co., LLC		CIP
NCR07011	Astoria Gas Turbine Power LLC		CIP
NCR07055	Cross Sound Cable Company, LLC		CIP
NCR07128	National Grid Generation LLC		CIP

2017 Compliance Audit Plan Off-Site			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR07136	Massachusetts Municipal Wholesale Electric Co		CIP
NCR07141	Middletown Power LLC		CIP
NCR07220	TransCanada Hydro Northeast Inc.		CIP
NCR10011	Covanta SEMASS		CIP
NCR10049	FirstLight Hydro Generating Company		CIP
NCR11243	NAES Corporation - MIRA - Jets		CIP
NCR11324	Brookfield White Pine Hydro, LLC		CIP
NCR11387	Allegany Generating Station LLC		CIP
NCR11459	Bucksport Generation LLC		CIP

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	Anticipated Date
Spring and Fall Workshops – NPCC holds semi-annual workshops as a primary mechanism for outreach to registered entities.	May 2017 November 2017
Introduction to NPCC for Beginners – NPCC provides an introductory class for those new to CMEP activities prior to the May and November workshops	May 2017 November 2017
Physical Security Outreach Program – This will focus on Transmission Owner's and Transmission Operator's transition to the new CIP-014 Physical Security standard.	Throughout 2017
Physical Security Information Exchange Sessions - The sessions take place at the May and November workshops and address NPCC Awareness Programs, Security Strategies, and subjects such CIP-014 implementation, and evolving physical threats to the electric industry.	May 2017 November 2017
Internal Controls Evaluation (ICE) Outreach Session – The sessions will take place at the May and November workshops to provide awareness and promote participation in the program. It will provide NPCC's purpose, approach and implementation of the voluntary ICE process, including expectations, tools, education/examples, best practices, deliverables, and feedback into Risk Based CMEP.	May 2017 November 2017
Cyber Security Outreach Program – This will provide guidance to NPCC registered entities that own Low Impact facilities under CIP Version 5 transition.	Throughout 2017
Individual Meetings with Registered Entities – NPCC will meet with registered entities for specific CMEP related issues if requested and warranted.	
CDAA – NPCC will issue announcements via CDAA (the NPCC Compliance Portal) informing registered entities of CMEP aspects.	
Compliance Wiki - NPCC's compliance wiki provides outreach specific to CDAA and other related issues and questions.	
Webinars – NPCC will conduct CMEP related webinars as needed. NPCC conducts pre-ICE webinars for all participants.	
FAQs – NPCC will post FAQs on an as needed basis	

Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Compliance Guidance Statements – NPCC may issue Compliance Guidance Statements to offer clarification on the compliance approach associated with the NERC Rules of Procedure, NERC Reliability Standards, or NPCC Regional Reliability Standards.	
Registered Entity Surveys – NPCC will issue surveys to registered entities on an as needed basis. Such surveys have included acquiring registration data, BES element data, workshop content preferences, etc.	
Website – The NPCC website provides information in the areas of Standards, Registration, Compliance Monitoring, and Compliance Enforcement.	

Appendix A4: ReliabilityFirst Corporation (ReliabilityFirst) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the ReliabilityFirst as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

ReliabilityFirst will follow and perform the Electric Reliability Organization (ERO) Risk-based Compliance Oversight Framework described in the ERO Compliance Monitoring Enforcement Program (CMEP) Implementation Plan. The 2017 ERO CMEP IP identifies a number of risk elements and areas of focus, which provide a starting point for ReliabilityFirst's risk analysis and Compliance Oversight Plan (COP) development. However, the 2017 ERO CMEP IP recognizes that it does not include the complete set of the risks that may affect the bulk power system (BPS) and that Regional Entities are expected to consider local risks and specific circumstances associated with individual registered entities within their footprint when developing their COPs.

As such, as set forth in more detail in Section 3, ReliabilityFirst performed its Regional Risk Assessment (RRA), which identified risks within the ReliabilityFirst region. ReliabilityFirst may monitor the Reliability Standards (Standards) and Requirements associated with these risks, which are referred to as the 2017 ReliabilityFirst Risk Elements, in 2017. ReliabilityFirst also has the discretion to add, subtract, or modify Standards and Requirements in its COPs for individual registered entities as it deems necessary based on the individual registered entity Inherent Risk Assessments (IRA) and COP development. The ReliabilityFirst RRA is discussed in further detail in Section 2 of this document.

ReliabilityFirst monitors Federal Energy Regulatory Commission (FERC) and NERC activities, system events, and events in the ReliabilityFirst region. Based on these monitoring activities, ReliabilityFirst may modify its CMEP IP throughout the year to address and mitigate situational awareness and reliability issues as they arise.

Other Regional Key Initiatives & Activities

Guided Self-Certifications

ReliabilityFirst will perform guided self-certifications as needed throughout in 2017. The guided self-certifications for a registered entity will be based upon the specific COP resulting from the registered entity's IRA and identification of any potential ERO-wide or regional risks. Guided self-certifications focus on specific risks and/or issues, and will require the registered entity to submit substantiating evidence to support its determination.

Risk-based Enforcement

ReliabilityFirst will continue to use a risk-based enforcement approach consistent with the ERO Enterprise. Specifically, ReliabilityFirst will exercise enforcement discretion by processing qualified minimal risk issues as "compliance exceptions." Compliance Exceptions will effectively supersede the Find, Fix, Track and Report ("FFT") disposition method for most minimal risk noncompliances. However, ReliabilityFirst will continue to use the FFT disposition method for moderate risk issues or minimal risk issues that ReliabilityFirst determines are otherwise inappropriate for compliance exception treatment.

The main difference between compliance exceptions and FFTs is that compliance exceptions do not aggravate a penalty for a future noncompliance by creating a formal violation history. There are two ways in which a minimal risk noncompliance may qualify for compliance exception treatment: (1) on a case-by-case basis and (2) via self-logging privileges that ReliabilityFirst grants to a registered entity based on the registered entity's demonstrated

ability to identify, assess, and correct noncompliances in addition to other factors. Case-by-case compliance exceptions are based on the facts and circumstances of a particular noncompliance. Self-logging privileges allow the presumption of compliance exception treatment for self-identified minimal risk issues for which the registered entity has earned the presumption.

Self-Logging

Self-logging allows qualified registered entities to keep a log of minimal risk noncompliances that ReliabilityFirst periodically checks in lieu of submitting individual self-reports and corresponding mitigation plans for each noncompliance. For each logged noncompliance, the registered entity records a detailed description of the facts and circumstances, the basis of the minimal risk assessment, and the associated mitigating activities. The registered entity submits the log to ReliabilityFirst for review and approval every three months. ReliabilityFirst checks the log to ensure that the noncompliance is sufficiently described, the minimal risk determination is justified and reasonable, and the mitigation is appropriate and adequate. After ReliabilityFirst approves the log entries, they are processed as compliance exceptions.

Logging privileges are awarded based on ReliabilityFirst's historic interactions with the registered entity, combined with ReliabilityFirst's evaluation of the registered entity's current ability to identify, assess, and correct noncompliances (an evaluation that is scaled based on the risk posed by the particular registered entity). With respect to historic interactions, ReliabilityFirst will consider: (1) the registered entity's compliance history and level of cooperation in prior compliance matters, (2) the registered entity's history of self-assessment, self-reporting, and timely and thorough mitigation, and (3) the quality, comprehensiveness, and execution of the registered entity's internal compliance program. For most Registered Entities, this is information that is already available to ReliabilityFirst.

A registered entity's current practices to identify, assess, and correct noncompliances is important to the analysis because self-logging relies on the registered entity's ability to properly arrive at its minimal risk determinations. In a traditional self-reported enforcement action, ReliabilityFirst does its own risk analysis and makes its decision about how to treat the violation based on that analysis. For ReliabilityFirst to allow the presumption of compliance exception treatment for minimal risk issues for which a registered entity is awarded self-logging privileges, ReliabilityFirst must have adequate assurance that the registered rntity has processes in place to identify, assess and correct noncompliances. In some circumstances, this information may also already be available to ReliabilityFirst through prior dealings with a registered entity. If it is not already available, ReliabilityFirst may request that information through interviews and documentation. One way to provide that information, and also potentially reduce audit scope, is to have ReliabilityFirst's Entity Development team conduct an internal controls evaluation focused on risk management. However, an internal controls evaluation is not required for ReliabilityFirst to award self-logging privileges.

ReliabilityFirst also requires self-logging entities to undergo training in Risk Harm Assessment and Estimating Uncertainties. This is a training that is offered periodically on-site at ReliabilityFirst, or ReliabilityFirst staff members can conduct training at the registered entity's facilities. This training provides an overview of how ReliabilityFirst makes its risk assessments. A registered entity is not required to adopt this methodology, but ReliabilityFirst has found that this training is a key component to ensuring justified and reasonable risk assessments on the registered entity's log. It is also helpful for resolving noncompliances that do not qualify for self-logging, because it creates a common understanding between the Registered Entity and ReliabilityFirst regarding risk analysis.

Regional Risk Assessment Process

The RRA identifies risks within the ReliabilityFirst region that could potentially impact the reliability of the BPS. To accomplish the RRA, ReliabilityFirst utilizes a cross-functional team of internal Subject Matter Experts (the RRA Team) to review and analyze information and data to determine the highest-priority risks to the ReliabilityFirst

region. The types of region-specific information and data the RRA Team reviews includes, but is not limited to: US Population & Census Data, Severe Weather Related Outages (*e.g.,* OE-417 reports, Outages), Generation Availability Data System (GADs), Transmissions Availability Data System (TADS), Misoperations, Event Analysis, Load Analysis, Locational Marginal Pricing, System Operating Limits (SOL), Interconnection Reliability Operating Limits (IROL), TIER Power Line Ranking, Interconnection Points, Cyber Security data, Physical Security data, and data on Threats and Vulnerabilities. After a period of information gathering, analysis and decision making, the RRA team develops the results of the RRA in the form of ReliabilityFirst Risk Elements.

Section 3 of this document contains additional detail on the ReliabilityFirst Risk Elements and their associated Standards and Requirements, which ReliabilityFirst may include in the 2017 registered entity-specific COPs.

The RRA is performed annually, but may be updated more frequently as necessary. As new and emerging threats and risks are identified, system events take place, and compliance monitoring activities are performed, ReliabilityFirst will update the RRA to keep current with potential issues, threats, and risks.

ReliabilityFirst reviews the potential risks to the reliability of the BPS posed by an individual registered entity by utilizing ERO IRA guidance and the associated internal IRA procedure to perform the registered entity IRA. This assessment and the COP development process help identify the areas of focus and the level of compliance oversight required for each registered entity.

The output from the IRA and COP development yields a COP (containing the scope of Standards and Requirements, monitoring interval, and CMEP tools – audit, spot check, or guided self-certification), which is shared with the registered entity via the IRA Summary Report included within the ReliabilityFirst Compliance Engagement notification package. Going forward, ReliabilityFirst will continue to complete an IRA and COP for each registered entity on the annual Critical Infrastructure Program (CIP) and Operations and Planning (O&P) compliance monitoring schedules. However, an IRA and COP may also be completed in response to new emerging risks or if a registered entity undergoes changes that may impact its risk to the BPS.

In addition to the Risk Elements and focus areas identified in the RRA, ReliabilityFirst considers the following Risk Factors when conducting an IRA (set forth in Appendix C to the 2014 ERO Inherent Risk Assessment Guide): *functional registered responsibilities, system geography, peak load and capacity, BPS exposure, interconnection points and critical path/IROLs, special protection systems/UVLS/UFLS, SCADA and EMS, System restoration responsibilities, system events and trends, compliance history and trends, culture of compliance, and overall composition.* In 2017, ReliabilityFirst will transition to using a new group of Risk Factors developed by and used across the ERO Enterprise (set forth in an Appendix to the new "ERO Enterprise Guide for Risk based Compliance Monitoring" due to release in Q4-2016): *UFLS Equipment, UFLS Development and Coordination, UVLS, Load, Transmission Portfolio, Voltage Control, Largest Generator Facility, Variable Generation, Total Generation Capacity, Planned Facilities, CIP Control Center Influence, CIP Connectivity, Critical Transmission, BA Coordination, RAS/SPS, Workforce Capability, Monitoring and Situational Awareness Tools, and System Restoration.*

ReliabilityFirst also analyzes various quantitative and qualitative considerations when developing the COP including, but not limited to:

- Population and Geographic Location
- Entity Make-up and Diversity
- Entity Registration
- Transmission Assets
- Misoperations

- Special Protection Schemes and Relay Protection
- Emergency Operations and Blackstart Facilities
- Generation Assets
- EMS and Monitoring Tools Availability
- Operating Performance
- Compliance History
- Normal System Performance
- System Maintenance Upkeep and Replacement

Additionally, where ReliabilityFirst has confidence in a registered entity's internal compliance program as a result of positive performance on an Internal Control Evaluation (ICE), ReliabilityFirst may narrow the audit scope and audit periodicity to reflect the compliance maturity of the registered entity. To support a strong culture of compliance and to demonstrate robust internal controls, registered entities are encouraged to continually perform self-assessments of their compliance programs and internal controls on an ongoing basis.

ReliabilityFirst will notify registered entities of the Reliability Standards and Requirements for which they will be monitored via any of the following means; posting of the Compliance Monitoring Schedule for Data Submittals; the audit notification letter; the spot check notification letter; the guided Self-Certification notification; and the IRA report which address the registered entity's tailored COP.

Regional Risk Elements and Areas of Focus

The 2016 ReliabilityFirst RRA identified the following 2017 ReliabilityFirst Risk Elements (in no particular order or ranking), which align with the 2017 ERO Risk Elements and therefore constitute Expanded ERO Risk Elements:

- Critical Infrastructure Protection
- Extreme Physical Events
- Maintenance and Management of BPS Assets
- Monitoring and Situational Awareness
- Protection System Failures
- Event Response / Recovery
- Planning and System Analysis
- Human Performance

The table below contains the Regional risk elements that ReliabilityFirst identified during the RRA process. Also, as a result of ReliabilityFirst's review of the NERC risk elements and the ReliabilityFirst risk elements, ReliabilityFirst identified the associated Standards and Requirements, listed below, for increased compliance monitoring focus in 2017. Thus, ReliabilityFirst justified the inclusion of these Standards and Requirements during the RRA. In the table below, ReliabilityFirst provides *additional justifications where applicable.* These Standards and Requirements will be considered as part of the IRA and COP development and may or may not be included in the registered entity-specific COP.

NOTE: Standards and/or Requirements in BLUE denote their inclusion in both the *ReliabilityFirst CMEP IP Appendix* and *2017 ERO CMEP IP*.

Table A4: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element(s)	**Justification**	**Associated Standard(s) & Requirement(s)**
Extreme Physical Events: - Extreme Natural Events Event Response/Recovery	ReliabilityFirst is expanding the ERO risk element(s) because, although entities made improvements, extreme cold weather conditions continued to impact unit performance. During site visits, although ReliabilityFirst determined that while the 2015-2016 generator winter performance improvements were effective, some of the short-term measures that Registered Entities implemented could be further improved to ensure that long-term generation performance improvements are sustained on a dependable basis. ReliabilityFirst found that while short-term solutions worked in some instances, in other instances, longer-term solutions are still necessary. Attachment 1-TOP-005 lists the types of data that Balancing Authorities and Transmission Operators are expected to share with other Balancing Authorities and Transmission Operators: Item 2. Other operating information updated as soon as available. *** Item 2.8. Severe weather, fire, or earthquake. There is demonstrated need to ensure that the conditions in Item 2.8 are met per R2.	EOP-001-2.1b R4 TOP-005-2a R2 TOP-002-2.1b R6-R7,R14-R15 TPL-001-4 R2
Extreme Physical Events: - Extreme Natural Events Maintenance and Management of BPS Assets Monitoring and Situational Awareness Event Response/Recovery Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) as a result of strained operating conditions in RF's footprint during unusually hot weather conditions and extreme cold weather conditions. Although the RF footprint experienced a milder winter in 2015-2016, the following remain important considerations for winter preparedness activities: (1) ensure processes are adequate for unit testing and preparation of resources in advance of winter operations, including testing dual-fuel capability; (2) review operator communications with respect to fuel-limited generation commitment decisions for accuracy and consistency; (3) make process changes as necessary to allow adjustment of start times based on changes in fuel utilized; (4) ensure requirements are met for generation units for which primary fuel may not be natural gas but that require gas to operate; (5) review emergency procedures to ensure effective communication and coordination of emergency	EOP-001-2.1b R2, R4 EOP-003-2 R1, R3, R5, R8 EOP-005-2 R1, R1.2 FAC-011-2 R3 FAC-014-2 R1-R2 IRO-001-1 R8 IRO-002-2 R4-R5 IRO-005-3.1a R12 IRO-008-1 R1-R2 IRO-009-2 R2-R3 NUC-001-3 R4 PER-005-2 R1-R2 TOP-001-1a R4-R5 TOP-002-2.1b R5-R7, R11, R15 TOP-004-2 R1 TOP-006-2 R5 VAR-001-4 R2

	procedures; (6) ensure transmission owners understand their existing voltage reduction capabilities (amount, time frame, etc.); and (7) consider adjustments to the roles and responsibilities for communications during emergency procedures other than refining the training to reinforce processes and tools. Regarding hot weather conditions, the ReliabilityFirst footprint experienced several days of unusual, extremely hot weather in September 2013 that led to emergency conditions in a Reliability Coordinator service area. During this period, temperatures were approximately 20 degrees above normal, and demand for electricity reached an all-time high. At the same time, some generation and transmission facilities were scheduled out of service for routine maintenance because lower system demand was usually experienced during this period. In order to avoid more serious impacts, the Reliability Coordinator had to direct Transmission Owners to implement controlled outages in a few contained areas for limited time periods. Controlled outages such as these are a last resort to prevent uncontrolled blackouts over larger areas. During a previous hurricane event, some TO and DP entities, particularly those that were not on the coast, experienced serious damage. For one entity, all service areas were impacted. The majority of increased staffing during this event occurred in the restoration area. Another entity, a nuclear facility, experienced a temporary loss of off-site power due to switchyard damage and a bushing on a voltage regulator associated with a transformer. During loss of off-site power at this facility, the reactor shutdown cooling and spent fuel cooling was temporarily lost, but was restored when emergency diesels started and loaded. Fossil units were forced off both pre-storm (in anticipation of potential flooding) and as the stations flooded. Five potential lessons learned were identified for generation stations during the storm. In addition to the lessons learned, several generation operation risks and challenges were also identified.	

Event Response/Recovery Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) because Transmission Operators' restoration plans and their resiliency must be constantly monitored to assure recovery plans are in place. ReliabilityFirst has identified this need as unique to its footprint as a result of the nature and size of the Transmission Operators in the ReliabilityFirst footprint. EOP-005-2, R6 focuses on verifying that the Transmission Operator's restoration plan accomplishes its intended function and that each Blackstart Resource is capable of meeting the requirements of its restoration plan. Overall, ensuring that large Transmission Operators meet these Requirements is essential to maintaining effective restoration plans.	EOP-005-2 R6
Extreme Physical Events: - Extreme Natural Events	ReliabilityFirst is expanding the ERO risk element(s) because the ReliabilityFirst Region can experience Geomagnetic Disturbance (GMD) events. GMD events can result in the loss of power transformers, loss of Reactive Power sources, increased Reactive Power demand, Misoperations, or other events. These may result in thermal overloads, equipment failures, and voltage collapse. Establishing requirements for Transmission system planned performance during GMD events is critical to the reliable operation of the BPS. Monitoring the readiness of the applicable entities is required to mitigate this potential risk.	TPL-007-1 R1-R7 - Effective dates staggered over 5 year period.
Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) because, with the role of the Planning Authority, Planning Coordinator, and Transmission Planner assuming more responsibility and authority in order to maintain system reliability, ensuring they are performing their role is critical to system reliability. TPL-001-4 ensures that system performance requirements are established for use by the Planning Authority and Planning Coordinator and Transmission Planners. ReliabilityFirst has determined that because of the nature of its footprint, with two large Planning Authorities and Planning Coordinators working in conjunction with the Transmission Planners, and the compliance monitoring history relating to TPL-001-4, evaluating these entities to these Requirements is essential to ensure that the system will operate reliably over a wide range of system conditions and probable contingencies.	TPL-001-4 R2-R3

Event Response/Recovery Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) because coordinated operation and actions across the ReliabilityFirst Region is critical due to the compact nature of the grid in the ReliabilityFirst Region. The emergency, interconnection, planning, transmission and generator operations standards ensure that the respective entities develop, maintain, and perform plans to maintain reliable operation, mitigate emergencies, and meet system performance requirements. The entities within the ReliabilityFirst Region must be evaluated to ensure they coordinate any actions with other entities besides conducting next-day analyses for anticipated normal and contingency conditions.	EOP-001-2.1b R1-R3, R4, R6 EOP-002-3.1 R1-R3, R4, R5 EOP-003-2 R1, R3, R7-R8 EOP-004-2 R2 IRO-003-2 R1-R2 IRO-004-2 R1 IRO-005-3.1a R5-R6, R9 PRC-006-1 R1-R5, R9-R10 PRC-022-1 R1 TOP-006-2 R2,R6-R7 TOP-007-0 R1-R4 TOP-008-1 R1-R4 TPL-001-4 R1-R3,R7 VAR-002-4 R2-R4
Human Performance	ReliabilityFirst is expanding the ERO risk element(s) because human performance and human interaction with critical elements on the BPS attributed to system operating issues in the ReliabilityFirst footprint. Due to human performance being a root cause of many noncompliances in the ReliabilityFirst footprint, Entities in the ReliabilityFirst region should understand that any operating condition that has not been studied or analyzed and where no valid operating limits exist is considered an unknown operating state and could negatively impact the reliability of the BPS. As an example, in one case, a switching event occurred when a line disconnect was closed into grounds on a 230 kV circuit which also resulted in the loss of generation.	FAC-010-2.1 R2.2 IRO-010-2 R2-R3 TOP-002-2.1b R6 TOP-004-2 R4
Maintenance and Management of BPS AssetsHuman Performance	ReliabilityFirst is expanding the ERO-risk element(s) because entities continue to experience issues regarding maintenance and testing of Protection System Devices since PRC-005 remains one of the most violated standard in the RF footprint.	PRC-005-6 R1,R2,R3,R4,R5
Human Performance	ReliabilityFirst is expanding the ERO risk element(s) because Generator Operators continue to experience deviations in voltage schedules and sometimes fail to notify the Transmission Operators since VAR-002 remains one of the most violated standards in the RF footprint. The root causes of these deviations and notice failures vary.	VAR-002-4 R1-R3 PER-005-2 R6
Event Response/Recovery Human Performance	ReliabilityFirst is expanding the ERO risk element(s) because Registered Entities within the ReliabilityFirst footprint have had varying issues with these Standards and Requirements and there have been and continues to	COM-002-4 R1-R4 EOP-001-2.1b R2-R4 EOP-003-2 R8 EOP-005-2 R10-R11, R17 EOP-006-2 R9-R10

	be changes of restoration resources, which require restoration plan updates.	
Protection System Failures Maintenance & Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) because the history of issues in the ReliabilityFirst region relating to protection system failures warrants increased focus.	FAC-010-2.1 R2.2 PRC-001-1.1(ii) R2, R2.2 PRC-004-4(i) R1,R2,R3,R4,R5,R6
Maintenance and Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) because Registered Entities in the ReliabilityFirst region have experienced various issues with energy management systems, Supervisory Control and Data Acquisition systems, ICCP, Contingency Analysis or State Estimators due to variations of these type of issues being experienced since 2014.	TOP-006-2 R1,R2
Maintenance and Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) because some entities in the ReliabilityFirst region have experienced equipment failures, some of which are maintenance related, and therefore increased focus is warranted. As an example, a Registered Entity experienced a phase to ground fault on a 230 kV circuit. The fault was due to the failure of a surge arrester. However, because of two protection equipment failures which were unrelated to each other, no tripping occurred. The fault persisted for a total of 58 seconds, eventually clearing as a result of backup ground protection on two 500 kV lines. This sustained fault resulted in the tripping of generators in the local area, and a severe voltage depression leading to a total load loss of approximately 532MW.	FAC-003-3 R1,R2,R3,R4,R5,R6,R7 PRC-005-6 R3-R4 PRC-008-0 R1-R2 PRC-011-0 R1 PRC-017-0 R1

Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) because, with the EPA Clean Power Plan resulting in the retirement of a number of generating facilities within ReliabilityFirst's footprint, additional focus is needed. The following additional justification is provided. The EPA Clean Power Plan may result in the retirement of generating facilities within the ReliabilityFirst region that cannot meet the environmental restrictions. Understanding the possible impacts early in the process is essential in order to inform decision- making and ensure that grid reliability is maintained. The Regional Transmission Operators and Independent System Operators in the ReliabilityFirst footprint have conducted reliability analyses to determine operating reserve and transmission needs resulting from potential generator retirements. With reserve margins in MISO's footprint already in decline due to Mercury and Air Toxics Standards and other factors, carbon-intensive generation retired for the purposes of complying with the EPA's proposal will need to be replaced fairly quickly.	BAL-002-1 R1 EOP-002-3.1 R2, R4 IRO-005-3.1a R2 TPL-001-4 R1-R2 VAR-001-4 R2
Critical Infrastructure Protection: - System Downtime Event Response/Recovery (With a focus on RESILIENCY)	ReliabilityFirst is expanding the ERO risk element(s) because resiliency in the ReliabilityFirst region continues to be of great importance to ReliabilityFirst, therefore increased focus is warranted. Within the region, there have been and continues to be changes of restoration resources, which require restoration plan updates. The following additional justification is provided.Per FERC's 2014-2015 Restoration Initiative focusing on black start restoration efforts, drills, training, ReliabilityFirst identified EOP-005, EOP-006, CIP-008-5 & CIP-009-6. Furthermore, CIP-008-5 requires an Incident Response Plan for Critical Cyber Assets. Lack of such a plan, in the event of an incident, will leave the entity with the inability to properly respond to the incident.* CIP-009-6 stipulates the requirements for backup and storage of information required to recover BES Cyber System functionality. It is crucial to timely recover BES Cyber Systems responsible for ensuring stability, operability, and reliability of the BES. * CIP-014 focuses on identifying and protecting Transmission stations and Transmission substations, and their associated primary control centers. If these are rendered inoperable or damaged as a result of a physical attack, this could result in instability, uncontrolled separation, or Cascading within an Interconnection.	EOP-005-2 R10-R11,R17 EOP-006-2 R9-R10 CIP-008-5 R1-R3 CIP-009-6 R1-R3 CIP-014-2 R1,R2,R3,R4,R5,R6

Monitoring and Situational Awareness	ReliabilityFirst is expanding the ERO risk element(s) because Registered Entities in the ReliabilityFirst region have had issues in this area as identified through the Event Analysis process and noncompliance dispositions, therefore warranting increased focus. This risk area considers loss of remote terminal units, energy management system outages, Supervisory Control and Data Acquisition issues, and loss of contingency analysis capabilities, ICCP, State Estimator, and Nonconvergence.	EOP-004-2 R2 EOP-008-1 R1 TOP-004-2 R4 TOP-006-2 R1-R2,R5
Maintenance & Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) because verifying the coordination of generating unit Facility or synchronous condenser voltage regulating controls, limit functions, equipment capabilities and Protection System settings is necessary for reliable operation of the BPS. Ensuring the availability of accurate information on generator Real and Reactive Power capability and synchronous condenser Reactive Power capability is essential for the modeling, analysis, and reliable operation of the BPS.	MOD-025-2 R1, R2, R3 PRC-019-2 R1, R2
Maintenance & Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) because of a deficiency in facility ratings methodologies and the impact of that deficiency on studies that rely on facility rating data. This risk element ensures that Facility Ratings are consistent with the registered entity's Facility Ratings methodology that is used in the reliable planning and operation. RF has identified inconsistences with Facility Ratings in operations and during monitoring engagements of registered entities.	FAC-008-3 R1,R2
Critical Infrastructure Protection: - System Downtime - Unauthorized Access	ReliabilityFirst is expanding the ERO risk element(s) because Registered Entities within the ReliabilityFirst footprint have had varying issues with these Standards and Requirements that warrant increased focus. Furthermore, NERC notes, events involving a complete loss of SCADA control, or monitoring functionality for 30 minutes or more, are the most common grid-related events since 2012 and limit the situational awareness of operators. Less-than-adequate situational awareness has the potential for significant negative reliability consequences and is often a precursor event or contributor to events. Additionally, insufficient communication and data regarding neighboring entities' operations could result in invalid assumptions of another system's behavior or system state. Considering that, the CIP standards that are related to deter, detect, or prevent malicious activity, event logging and monitoring, access control are included.	CIP-003-6 R1, Part 1.1 CIP-004-6 R1-R5 CIP-005-5 R1-R2 CIP-006-6 R1-R2 CIP-007-6 R1,R2,R3,R4,R5 CIP-011-2 R1-R2

Critical Infrastructure Protection: Extreme Physical Events: - Physical Security Vulnerabilities	ReliabilityFirst is expanding the ERO risk element(s) because CIP-006 is a widely violated standard in the ReliabilityFirst Region. Also, CIP-014 is a newly released standard focused on protections of Transmission stations and substations, and their associated primary control centers. Thus, additional focus is needed to address and minimize both the magnitude and duration of the consequences of physical events or attacks. Furthermore, physical access to cyber systems must be restricted and appropriately managed to ensure the integrity of the cyber systems within the Physical Security Perimeter. Failure to comply with the requirements of these standards can lead to threats in physical security space.	CIP-006-6 R1-R3 CIP-014-2 R1,R2,R3,R4,R5,R6
Critical Infrastructure Protection: - Corruption of Operational Data	ReliabilityFirst is expanding this ERO risk element(s) because Registered Entities within the ReliabilityFirst footprint have had varying issues with the v3 equivalent Standards and Requirements and therefore these warrant increased focus. * CIP-009-6 R1-R3 requires a recovery plan for Critical Cyber Assets. Lack of such a plan, in the event of equipment failure, will leave the entity with the inability to properly recover from an event. * CIP-010-2 R1-R2 deal with having processes for Change Control and Configuration Management of Critical Cyber Asset hardware and software. Lack of such processes, in the event of equipment failure, will leave the entity with the inability to properly recover from an event. Failure to document and implement a viable Change Control and Configuration Management program that helps assure the correct and timely restoration of CCAs could have a very negative impact on the availability and security of the BES. * CIP-010-2 R3-R4 deal with vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.	CIP-009-6 R1-R3 CIP-010-2 R1-R4
Critical Infrastructure Protection: - BES System categorization Impact rating	ReliabilityFirst is expanding the ERO risk element(s) because in CIP-002-5.1, identification and accurate categorization of BES Cyber Systems and their associated BES Cyber Assets are crucial. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.	CIP-002-5.1 R1-R2

Critical Infrastructure Protection: - Low Impact BES Cyber Systems	ReliabilityFirst is expanding the ERO risk element(s) because the inclusion of CIP-003-6 and its identified Requirements triggers RF to monitor Registered Entities who may declare only Low Impact BES Cyber Systems. These Registered Entities provide a new risk to the BES as many may never have had full CIP scope under previous versions of the CIP Standards. This is a potential risk as these entities may have less mature CIP Programs including implementation of required cyber and physical security controls. The Low Impact BES Cyber Systems for these new in scope entities will most likely be at transmission substations or stations and/or generation stations.	CIP-003-6 R1, Part 1.2-R4

Regional Compliance Monitoring Plan

This section includes regional risk-based CMEP activities. Following is an overview of the year's currently known IRA, audit, spot check, periodic data submittals, and self-certifications. The audit schedule is also located on the ReliabilityFirst's website here: https://www.rfirst.org/compliance/Pages/Schedules.aspx

CIP Compliance Monitoring Plan

ReliabilityFirst intends to conduct 11 on-site CIP Audits in 2017, and may conduct additional audits as necessary. Most of the 11 audits are being conducted pursuant to the ROP and include registered entities that must be audited every three years. Other audits are scheduled as a result of IRAs, Enforcement Actions, and/or Entity Programs new to CIP V5 applicability. Five of the 11 audits are Multi-Region Registered Entity (MRRE) engagements, and ReliabilityFirst is the Lead Regional Entity for four of these audits. ReliabilityFirst is developing the scope for these audits through its IRA process. ReliabilityFirst has already contacted the registered entities being audited in 2017 to arrange schedules and confirm the audit engagements.

Operations and Planning Compliance Monitoring Plan

ReliabilityFirst intends to conduct 60 Operations and Planning engagements in 2017, but may conduct additional engagements as necessary. These engagements are being conducted pursuant to theROP and include registered entities that must be audited every three years. Six of the 60 audits are MRRE engagements in which two will be led by another Regional Entity. ReliabilityFirst has already contacted the registered entities being audited in 2017 to arrange schedules and confirm the audit engagements.

Inherent Risk Assessments

ReliabilityFirst will schedule and perform IRAs for each registered entity based upon the CIP and O&P audit schedules. However, this schedule and the IRAs themselves may be revised based on emerging risks, a Registered Entity's performance that requires Regional attention, or any other changes to a Registered Entity or otherwise that may impact a registered entity's risk to the BPS.

Once ReliabilityFirst completes an IRA, it establishes a registered entity-specific, customized COP which addresses the compliance monitoring scope, frequency, and the CMEP tool(s) (*e.g.,* audit, spot check, or self-certification) that will be used to monitor the registered entity. Based on the results of the IRA, a registered entity's monitoring frequency may be adjusted, and as such adjustments are made, ReliabilityFirst will update the audit schedule. For registered entities for which ReliabilityFirst has not conducted an IRA, compliance monitoring will be targeted based upon the ERO and Region risks previously discussed. ReliabilityFirst will follow the CMEP timing and guidance found in Section 3 of Appendix 4C of the ROP to initiate this monitoring.

Self-Certifications

ReliabilityFirst will perform guided self-certifications (GSC) as needed throughout in 2017. The guided self-certifications will be based upon the Registered Entity's specific COP resulting from its IRA, a regional identified risk or as directed by NERC. Guided self-certifications will be focused on specific risks or issues and will require the registered entity to submit substantiating evidence to support its determination.

Tentatively planned GSCs for 2017 include:

- FAC-003-4
- TOP-003-3
- CIP-002-5.1 (Entities that only own Low assets based upon the impact rating criteria)
- CIP-003-6 (Entities that only own Low assets based upon the impact rating criteria)
- MOD-032-1

Spot Checks

ReliabilityFirst may schedule Spot Checks in 2017, and reserves the option to initiate Spot Checks throughout the year as needed. In addition, ReliabilityFirst may use the Spot Check process to verify mitigation plans as needed.

Periodic Data Submittals

ReliabilityFirst developed a Compliance Monitoring Schedule that contains the Standards and Requirements for the Periodic Data Submittals scheduled for 2017. Most of these data submittals are associated with the monthly, quarterly, and or annual reporting requirements set forth in the Requirements.

ReliabilityFirst's audit schedule will be posted on the ReliabilityFirst website, but is subject to change based upon each Registered Entity's IRA. If a registered entity has a question concerning its audit schedule, contact ReliabilityFirst.

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR00682 NCR01056 NCR11401	AEP Electric Power Service Corporation Companies (MRRE – RF Lead Region) AEP Generation Resources Inc.		CIP
NCR00006	Calpine (MRRE – Texas RE Lead Region)		CIP
NCR00718	City of Lansing Board of Water and Light		CIP
NCR00748 NCR00759	The Dayton Power and Light Company AES Ohio Generation, LLC		CIP
NCR00753	DTE Electric Company		CIP
NCR10161 NCR00129 NCR03034 NCR07087 NCR11287 NCR10375 NCR03006	EDPR Companies (MRRE – RF Lead Region)		CIP

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR11037 NCR11073 NCR11079 NCR03013 NCR11072 NCR08054 NCR10135 NCR11172 NCR11494 NCR06041 NCR06040 NCR03048 NCR11201 NCR10302 NCR04097 NCR10167 NCR10126 NCR11123 NCR10279 NCR10318 NCR11505 NCR11577 NCR11570			
NCR00374 NCR00540 NCR00212 NCR00251 NCR00168	Essential Power (MRRE – RF Lead Region)		CIP
NCR00798	Indianapolis Power and Light Company		CIP
NCR10400 NCR10192 NCR00803 NCR00820 NCR08023	ITC Companies (MRRE – RF Lead Region)		CIP
NCR04167	U.S. Department of Energy		CIP
NCR00762	Duquesne Light and Power Company		CIP
NCR00006	Calpine (MRRE – Texas RE Lead Region)	O&P	
NCR00711	City of Batavia Municipal Electric Utility	O&P	
NCR00716	City of Greenfield	O&P	
NCR08008	City of Jackson, Oh	O&P	
NCR11247	GSG 6, LLC	O&P	
NCR00721	City of Rochelle	O&P	
NCR00941	Washington City Light & Power	O&P	

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR06020	Wadsworth Electric & Communications	O&P	
NCR10257	EFS Parlin Holdings LLC	O&P	
NCR10305	EcoGrove Wind LLC	O&P	
NCR11228	Eagle Point Power Generation, LLC	O&P	
NCR11391	West Deptford Energy, LLC	O&P	
NCR00718	City of Lansing by its Board of Water and Light	O&P	
NCR04167	U.S. Department of Energy	O&P	
NCR00376	Forked River Power LLC	O&P	
NCR10308	Fowler Ridge III Wind Farm LLC	O&P	
NCR10306	Grand Ridge Energy LLC	O&P	
NCR11136	GenOn Power Midwest	O&P	
NCR11137	GenOn Northeast Management Company	O&P	
NCR11235	Gratiot County Wind LLC	O&P	
NCR11335	Interpower/Ahlcon Partners Limited Partnership	O&P	
NCR00796	Indiana Municipal Power Agency (RF Lead Region)	O&P	
NCR00753	DTE Electric Company	O&P	
NCR00852	Northampton Generating Company	O&P	
NCR10035	Napoleon Light & Power	O&P	
NCR10208	Lincoln Generating Facility, LLC	O&P	
NCR11311	Mehoopany Wind Energy LLC	O&P	
NCR11409	Michigan Power LP	O&P	
NCR00889	Susquehanna Nuclear	O&P	
NCR11308	Raven Power Holdings LLC	O&P	
NCR02611	Northern Indiana Public Service Company	O&P	
NCR08073	The City of Hamilton, Ohio	O&P	
NCR11280	Twin Ridges Wind Farm	O&P	
NCR11362	Talen Generation	O&P	
NCR00740	Consumers Energy Company	O&P	
NCR00748	The Dayton Power and Light Company	O&P	
NCR00893	PSEG Fossil LLC	O&P	
NCR00895	PSEG Nuclear LLC	O&P	
NCR11660	Rockford Generation, LLC	O&P	
NCR00690	Big Sandy Peaker Plant, LLC	O&P	
NCR00252	Calumet Energy Team, LLC	O&P	
NCR00214	Camp Grove Wind Farm, LLC	O&P	
NCR11289	Bishop Hill Energy LLC	O&P	
NCR00762	Duquesne Light Company	O&P	
NCR00718	City of Lansing Board of Water and Light	O&P	
NCR08014	Cuyahoga Falls Electric System	O&P	
NCR10161 NCR00129 NCR03034	EDPR Companies (MRRE – RF Lead Region)	O&P	

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR07087 NCR11287 NCR10375 NCR03006 NCR11037 NCR11073 NCR11079 NCR03013 NCR11072 NCR08054 NCR10135 NCR11172 NCR11494 NCR06041 NCR06040 NCR03048 NCR11201 NCR10302 NCR04097 NCR10167 NCR10126 NCR11123 NCR10279 NCR10318 NCR11505 NCR11577 NCR11570			
NCR00374 NCR00540 NCR00212 NCR00251 NCR00168	Essential Power (MRRE – RF Lead Region)	O&P	
NCR10400 NCR10192 NCR00803 NCR00820 NCR08023	ITC Companies (MRRE – RF Lead Region)	O&P	

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Monthly Newsletter - The ReliabilityFirst Newsletter provides Registered Entities with news and information relating to reliability activities.	Bi-Monthly throughout the year.
Monthly Compliance Update Letter - The ReliabilityFirst Monthly Compliance Update Letter provides Registered Entities with any changes made to the Compliance Monitoring Schedule and the due dates for compliance submittals.	Monthly throughout the year.
ReliabilityFirst Website - The ReliabilityFirst website provides compliance and technical materials to support compliance program performance.	Monthly throughout the year.
Workshops/Seminars/Webinars - ReliabilityFirst Reliability workshops/seminars or webinars will be scheduled to assist the Registered Entities in the understanding of their responsibilities to satisfy compliance to the Reliability Standards throughout the year.	Semi-annual (Baltimore: April 18-21, 2017 and Independence: September 26-29, 2017).
CIP Version 5 Outreach and Awareness – ReliabilityFirst will conduct CIP Version 5 outreach, including training and education engagements, to ensure that Registered Entities have confidence in their implementation of the CIP V5 Standards and Requirements. These engagements will primarily be conducted as Workshops and Webinars.	Multiple SRP type readiness assessments have been conducted at entity request. These assessments fall under the Assist visit umbrella.
Compliance Data Management System (CDMS) - ReliabilityFirst allows its Registered Entities to report compliance via CDMS, an internet based application. The CDMS home page provides informational announcements, updates, and newsworthy items of interest to the Registered Entities.	Updated throughout the year as needed.

Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Periodic Reports - ReliabilityFirst will provide Periodic Reports to its Registered Entities identifying compliance related activities that the Registered Entities continue to struggle with. These reports will be posted on the ReliabilityFirst website.	Monthly throughout the year. Reports have primarily come through newsletter articles. There have been at least two so far this year with topics such as "**Compliance Aspects of Organizational Transitions"**
Open Compliance Calls - ReliabilityFirst has instituted a monthly conference call to provide an open forum for Registered Entities to call and voice concerns, ask questions, and to gain information about upcoming compliance items.	Monthly throughout the year.
Assist Visits - ReliabilityFirst has instituted a program whereby a Registered Entity may request a one-on-one or small group meeting where guidance on compliance related activities can be provided. These Assist Visits can be in the form of a conference call, web meeting, or on-site visit. Topics can range from helping a Registered Entity become more familiar with compliance related material and activities, to special guidance and education when either the Registered Entity or ReliabilityFirst believes the Registered Entity needs special attention or additional help.	As requested by our registered entities. There have been 27 Assist Visits thus far in 2016 22 have been CIP v5 related. RF has collected survey responses for the entities that have participated in the program with an 85%+ positive rating. Multiple SRP type readiness assessments have been conducted at entity request. These assessments fall under the Assist visit umbrella.
MkInsight Entity Profile - ReliabilityFirst will allow its Registered Entities to report entity specific information, using an internet based application compliance monitoring application.	Updated throughout the year as needed.

Appendix A5 - SERC Reliability Corporation (SERC) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for SERC as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

NERC Compliance Monitoring Enforcement Program (CMEP) tools used by SERC in 2017 will include Compliance Audit, Spot Check, and Guided Self-Certification. SERC will focus its resources on higher risk items primarily identified through entity-specific Inherent Risk Assessments (IRA)s. SERC will continue to include an outreach component to on-site compliance audits. During the on-site week, the entity may engage SERC compliance audit staff to address approaches and ask questions in both the Operating and Planning (O&P) and Critical Infrastructure Protection (CIP) compliance areas. SERC has also improved the formality and timeliness of its Frequently Asked Questions process, where SERC Subject Matter Experts address questions asked by entities.

SERC continues to support its Industry Subject Matter Expert (ISME) program, in which SERC audit teams occasionally use volunteers employed by registered entities in the SERC Region as supplemental compliance audit team members for both O&P and CIP audits. The program approach focuses on identification, qualification, and assignment of ISMEs to match the technical resource needs of the specific compliance audits. Information about SERC's ISME program is available on the SERC website.

Other Regional Key Initiatives and Activities

SERC will continue to participate in the Multi-Regional Registered Entity (MRRE) program in 2017. As a Lead Regional Entity (LRE), SERC will lead efforts related to all aspects of the CMEP. The LRE coordinates and conducts the IRA, with input from each Affected Regional Entity (ARE), and determines the appropriate compliance monitoring approach. This coordinated oversight should eliminate unnecessary duplication of compliance monitoring and enforcement activities. In addition, as the ARE, SERC will collaborate with the LRE to ensure entity IRA, compliance monitoring, and enforcement activities include SERC regional considerations.

To help prevent unintended redundancy and gaps in responsibilities within the Transmission Operator (TOP) function, SERC will continue to give consideration to local (transmission) control centers. Because local control centers could perform some TOP tasks, SERC Compliance Monitoring will focus on certain aspects of reliability including but not limited to system restoration, protection system monitoring, operator training, and backup functionality. In 2017 SERC will perform focused CMEP activities involving certain local control centers.

The IRA and Internal Controls Evaluation (ICE) programs will continue to mature in 2017. In 2016, SERC focused on completing the IRAs on the Reliability Coordinators, Balancing Authorities, and Transmission Operators. In 2017, SERC will focus on the remaining entities with a goal of completing an IRA on all SERC registered entities by the end of the year. SERC will continue to develop a registered entity's compliance oversight plan based on the risks identified during the IRA process.

As part of the risk-based CMEP, SERC will periodically sample Compliance Exception mitigating activities. SERC will sample from the Compliance Exceptions filed with NERC, and where the mitigating activities completion date has passed. The mitigation verification may occur periodically by Entity Assessment and Mitigation staff or during scheduled Compliance Monitoring activities.

Regional Risk Assessment Process

Reliable operation of the bulk power system (BPS) is crucial. SERC recognizes that protecting the reliability of the electric grid in the SERC Region is the responsibility of its members with SERC's support. Achieving a secure and reliable grid requires registered entities to remain diligent about reliability and resiliency within their service areas. SERC is responsible for assisting registered entities in identifying regional reliability risks and coordinating reliability-related activities throughout the Region.

SERC has coordinated efforts with its stakeholders since 2012 to develop and implement a continuous program of regional assessment of potential reliability risks to the SERC Region BPS. The SERC Regional Reliability Risk Assessment program is a robust, centralized process for analyzing, prioritizing, addressing, and communicating significant risks and risk-controlled initiatives.

The program's objective is to improve BPS reliability through a coordinated effort of a cross-functional organization that identifies, analyzes, prioritizes, and addresses reliability risks. In conformance with the ERO risk-based CMEP, the SERC process consists of the following major activities:

- Identify or nominate risks.
- Determine time horizon (i.e., immediate, next-day, operational, seasonal, and long-term).
- Assess and rank risk:
  - Determine the consequence or severity impact(s).
  - Determine the probability of occurrence.
  - Assign High, Medium, or Low from the Risk Assessment Matrix.
  - Prioritize risks.
  - Store the information in the Risk Registry.
- Develop risk control initiatives.
- Monitor and reevaluate risk impact.

SERC's Reliability Risk Team (RRT) is a major participant in the program. The RRT is responsible for identifying risks based on the probability of occurrence and severity of impact. SERC's RRT identified three different areas of risk:

- Operational Risk(s)
- Engineering Risk(s)
- Critical Infrastructure Protection (CIP)

SERC also identified risk elements within each group. These identified risk elements align with the 2017 ERO-wide risk elements:

- Critical Infrastructure Protection
- Extreme Physical Events
- Monitoring and Situational Awareness
- Planning and System Analysis

As new and emerging threats and risks are identified, system events occur, and compliance monitoring activities are performed, SERC's RRT will update the regional Reliability Risk Assessment program to include current

potential issues, threats, and risks. In addition, as SERC performs IRAs of its registered entities, SERC will review potential risks to BPS reliability posed by individual registered entities.

The coordination among the SERC registered entities, SERC technical committees, SERC staff, neighboring system personnel, and other members of the ERO is vital to the understanding and analysis of potential major reliability issues. In 2015, SERC implemented its Integrated Risk Management (IRM) program. The IRM process addresses SERC's need to gather and analyze data to support risk-based techniques. SERC determined the best method to support this initiative is through uninhibited sharing of data across SERC program areas. The objective of the IRM is to support risk-based compliance monitoring and enforcement by defining and deploying sound business policies, procedures, and process tools across all SERC departments to implement a comprehensive integrated risk management program.

SERC, through its members and staff, is heavily engaged with NERC and its initiatives. SERC's risk management programs enable it to focus compliance monitoring oversight activities on those Reliability Standards which, if violated, would pose the greatest risk to the reliable operation of the SERC portion of the BPS.

Regional Risk Elements and Areas of Focus

The table below contains the Regional risk focus areas identified during the Regional Risk Assessment process. The table also contains areas of focus for each identified risk that may be considered in the development of the registered entity's compliance oversight plan.

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Cold Weather Impacts on Transmission and Generation	SERC is expanding the NERC risk element based on operational risks, such as deficient entity responses and performance, identified during cold weather events. It is important from an operational perspective to consider proper operation of the system during these events, with respect to balancing resources and demand, and necessary communication capabilities.	BAL-002-1 R1; BAL-005-0.2b R7; COM-002-4 R5, R6, R7; EOP-002-3.1 R3, R6, R7.
Major Storm Events	The SERC Region historically has experienced severe weather events, such as hurricanes and tornados. These events usually create system contingencies beyond existing planning criteria. However, emergency procedures and other operating standards still apply. Over the years, the Region has identified this risk and emphasized system preparedness through the 2012 Assessment of SERC Performance Information for Identifying Potential Reliability Risk, as well as through the NERC Reliability Assessment reporting process.	COM-002-4 R1, R2, R5, R6, R7; EOP-006-2 R1, R7, R8; EOP-008-1 R1, R2, R4, R7
Power System Coordination and Modeling	The following can introduce risk to the reliable operation of the BPS in the SERC Region: • Increased use of the BPS in a manner for which the system was not originally designed • Inadequate operating experience	MOD-001-1a R6; FAC-008-3 R6; FAC-014-2 R1, R2, R3, R4; IRO-003-2 R1, R2; IRO-004-2 R1; VAR-001-4 R1, R2;

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	• Insufficient coordinated studies • Insufficient coordinated operations SERC's unique Planning Coordinator structure necessitates coordination throughout the SERC Region. There are a large number of Planning Coordinators in the SERC Region who coordinate with multiple entities. Performing modeling without appropriate coordination would risk the validity of SERC study performance. In addition, the NERC Arizona-Southern California Outages Report highlighted potential areas of vulnerability. Significant changes in generation dispatch, particularly if such changes are unstudied, increase reliability risks. Such risks warrant additional focus on registered entities impacted by these issues with respect to these Standards. References to neighboring system coordination and recommendations can be found in the NERC Arizona-Southern California Outages Report.	VAR-002-4 R1, R2, R3
Underfrequency Load Shedding (UFLS) Schemes	The SERC UFLS Regional Standard is to establish consistent and coordinated requirements for the design, implementation, and analysis of UFLS programs among applicable SERC registered entities. The Regional Standard adds specificity not contained in the NERC Standard for development and implementation of the UFLS scheme in the SERC Region that effectively mitigates the consequences of an under-frequency event.	PRC-006-SERC-01 R1, R2, R3, R4, R5, R6
Maintenance and Management of BPS Assets	The SERC footprint is in a geographic area that has dense vegetation. Right-of-way inspections are important to identify potential vegetation issues that could pose a risk to the reliability of the transmission system.	FAC-003-3 R3, R6, R7

Regional Compliance Monitoring Plan

This section includes regional risk-based CMEP activities. Following is an overview of the year's currently known IRA, audit, spot check, periodic data submittals, and self-certifications. The audit schedule is also located on the SERC's website here: Compliance Monitoring

Inherent Risk Assessments

In 2017, SERC is on schedule to complete an IRA for each of its registered entities. However, the schedule may be revised based on emerging risks, a registered entity's performance, or any other significant changes to a registered entity that may impact a registered entity's risk to the BPS. SERC completes the IRA, then establishes a registered entity compliance oversight plan, which includes the compliance monitoring scope, frequency, and the CMEP tool(s) (e.g., audit, spot check, or self-certification) that may be used to monitor the registered entity. Based on

the IRA, a registered entity's monitoring frequency or CMEP tool may be adjusted, and as such adjustments are made, SERC will update the compliance monitoring schedule.

Compliance Audits

In accordance with NERC ROP, SERC will conduct on-site compliance audits at least every three years on those registered entities registered as a Reliability Coordinator, Balancing Authority, or TOP. This audit scope will be based on the results of each entity's IRA. The specific Standards and Requirements that compose the scope of the audit will be defined in the entity's Audit Detail Letter that is sent to the entity 90 days prior to the on-site week.

For a registered entity that is not scheduled for a three-year audit, SERC may perform an IRA and determine that a registered entity's inherent risk is large enough to justify additional compliance monitoring activity. Certain triggers could generate a targeted Compliance Audit or Spot Check. These triggers include but are not limited to events, misoperations, significant organizational changes, asset acquisitions, and so forth.

Spot Checks

Spot Checks in 2017 will be determined by the results of an entity's IRA, Mitigation Plan verification, events, or performance trends.

Guided Self-Certifications

The need for Guided Self-Certifications will be determined by the results of an entity's IRA. Usually, low-risk Standards and Requirements are the focus of the Guided Self-Certification monitoring method. Guided Self-Certification forms require the inclusion of supporting evidence to provide reasonable assurance of compliance, and could also include questions and data requests.

Periodic Data Submittals

Some Standards and Requirements require data submittal, which could be on a monthly, quarterly, or annual basis. An ERO-wide 2017 data submittal schedule will be posted on the SERC web site.

2017 Compliance Audit Plan

SERC registered entities listed in the 2017 Compliance Audit Plan include on-site and off-site audits.

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR10248	Ameren Missouri	O&P	CIP
NCR01175	Ameren Services Company	O&P	CIP
NCR11399	Electric Energy, Inc.	O&P	CIP
NCR01248	Georgia System Operations Corporation	O&P	CIP
NCR00915	South Carolina Electric & Gas Company	O&P	CIP
NCR01143	Southwest Power Pool		CIP
NCR01365	VACAR South	O&P	CIP
NCR11399	Electric Energy, Inc.	O&P	CIP
NCR01191	Central Electric Power Cooperative Inc.	O&P	
NCR01192	Citizens Electric Corporation	O&P	
NCR01225	East Kentucky Power Cooperative	O&P	
NCR01249	Georgia Transmission Corporation	O&P	CIP

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR01278	Municipal Electric Authority of Georgia	O&P	
NCR11077	Nashville Electric Service	O&P	
NCR09035	Prairie Power, Inc.	O&P	
NCR01214	Virginia Electric and Power Company	O&P	
NCR01273	Mississippi Power	O&P	
NCR01252	Gulf Power Company	O&P	
NCR01320	Southern Company Services, Inc. - Trans	O&P	
NCR01321	Southern Illinois Power Cooperative		CIP
NCR01177	Associated Electric Cooperative, Inc.		CIP

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	Anticipated Date
Outreach Events SERC outreach events occur throughout the year to accommodate the training and education needs of registered entities. Planned events, listed here, with specific themes will also feature compliance and reliability topics of importance at the time of the event. SERC staff post event details on the Upcoming Events page of the SERC website, which can be accessed through the Event Calendar on the home page or under Outreach > Events Calendar. Outreach events are promoted in the monthly *SERC Transmission* newsletter, and email notifications; and reminders are sent to primary and alternate compliance contacts for all registered entities within the SERC Region footprint. • Open Forum (WebEx) • Open Forum (WebEx): SERC 101 • Spring Compliance Seminar (Charlotte, NC and WebEx) • Small Entity Seminar • Open Forum (WebEx) • Open Forum (WebEx) • Fall Compliance Seminar (Charlotte, NC and WebEx) • CIP Compliance Seminar	Jan 30, 2017 Feb 6, 2017 Mar 28-29, 2017 Mar 29, 2017 May 22, 2017 Jul 31, 2017 Sep 19-20, 2017 Oct 31-Nov 1, 2017
Focused Workshops and Webinars Supplemental focused events scheduled on an as-needed basis provide outreach and training for new or revised Reliability Standards, targeted groups of registered entities based on functional registration, and ERO initiatives.	As needed throughout the year

Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
FAQ & Lessons Learned SERC staff subject matter experts address technical questions received from registered entities, then post them on the website, along with lessons learned to share information and best practices. Items are listed by topical categories and posted on the SERC website under Outreach / FAQ & Lessons Learned.	As available throughout the year
Compliance Outreach Assistance Upon receipt of a New Registration Application, SERC sends a document containing links to "Compliance 101" files on the FERC, NERC, and SERC websites to the applicant to provide basic compliance information in one convenient location. A sample of the links includes information such as the Energy Policy Act (EPA) of 2005 on the FERC site, ROP and Reliability Standards on the NERC site, and Acronym Reference Index and SERC Filing Due Dates on the SERC site. SERC distributes the *SERC Transmission* newsletter to registered entities within the SERC Region each month and posts it on the SERC website. Articles contain links to scheduled outreach information for both SERC and NERC events, along with other topics helpful to maintaining BPS reliability.	Updated as needed throughout the year
SERC Compliance Portal SERC registered entities submit Self-Certifications, Self-Reports, Mitigation Plans, and Data Submittals via the SERC Portal. Feedback from targeted surveys allow SERC to incorporate enhancements based on the needs of the users, and outreach events include training on upgrades and enhancements.	As needed throughout the year
Dedicated Email In-Boxes Appropriate SERC staff monitor dedicated email in-boxes established for questions from stakeholders. The Contact Us link is accessible from any page of the SERC website, and features a list of topics along with the email address link to submit questions. A sampling of the topics include CIP V5 transition, compliance issues, and situational awareness/events analysis.	Monitored throughout the year

Appendix A6 - Southwest Power Pool Regional Entity (SPP RE) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the SPP RE as required by the NERC Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- SPP RE Compliance staff will complete or refresh the Inherent Risk Assessment (IRA) for the registered entities that are on the 2017 monitoring schedule prior to the 2017 monitoring activity. Concurrent with each IRA the SPP RE Compliance Staff will determine the compliance oversight plans which includes the monitoring scope, interval of the engagement, and compliance monitoring method.
- SPP RE Critical Infrastructure Protection (CIP) monitoring will focus on registered entities with high, medium, and low impact Bulk Electric System (BES) Cyber Systems.
- Specific Reliability Standards require periodic data submittals. The SPP RE, SPP RTO, and MISO collect data submittals on a monthly, quarterly, or annual basis. To fulfill the requirements, registered entities will submit reports according to the 2017 periodic data submittal schedule as noted in the *Notice to Registered Entities of SPP RE 2017 Reporting Requirements Schedule. spp.org>Regional Entity Home>Compliance and Enforcement>2017 Compliance Documents*
- The SPP RE identified requirements that will be monitored through self-certification on either a quarterly or annual basis. The requirements and schedule are noted in the *Notice to Registered Entities of SPP RE 2017 Reporting Requirements Schedule. spp.org>Regional Entity Home>Compliance and Enforcement>2017 Compliance Documents*
- SPP RE will:
  - Continue to engage the registered entities that request an Internal Controls Evaluations (ICE) and Self-Logging.
  - Continue to implement the Coordinated Oversight Program (COP) for the Multi-Regional Registered Entities (MRREs).
  - Continue to develop and refine the tools and templates used for compliance monitoring, IRA, and ICE.
  - Perform internal reviews of compliance monitoring for the purpose of improving the SPP RE compliance oversight program.

Other Regional Key Initiatives and Activities

- SPP RE will continue to collaborate with NERC, Regional Entities, and the registered entities to identify changes to enhance the risk-based approach to monitoring and enforcement processes.

Regional Risk Assessment Process

- SPP RE developed a RE-specific risk element based on compliance findings in the SPP RE footprint, regional system events and SPP RE staff's professional judgement.
- SPP RE will consider these Regional risk focus areas when following the ERO Risk-based Compliance Oversight Framework described in the Electric Reliability Organization (ERO) Compliance Monitoring Enforcement Program (CMEP). SPP RE will also consider the Regional risk focus areas when conducting

risk assessments to develop the audit scope for the registered entities that are scheduled for audits during 2017.

Regional Risk Elements and Areas of Focus

The table below contains the Regional risk focus areas identified during the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of the registered entities compliance oversight plan.

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Voltage Support	SPP RE identified this risk element due to the number of Self-Reports indicating failure to maintain reactive support and voltage control. The purpose is to ensure generators provide reactive support and voltage control in order to protect equipment and maintain reliable operation.	VAR-002-4 R1, R2

Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Critical Infrastructure Protection	SPP RE is expanding this risk element based on the history that has shown malicious actors are often in a compromised system six to eighteen months before being detected. A robust event logging and monitoring program is essential to early detection. Similarly, it has been shown that approximately 80% of successful system compromises are enabled by poor patch management, poor anti-malware protections, and poor user access management.	CIP-007-6 R4 CIP-004-6 R6
Maintenance and Management of BPS Assets	SPP RE is expanding this risk element because of a deficiency in facility ratings methodologies and the impact of that deficiency on studies that rely on facility rating data. These risk elements ensure that Facility Ratings are consistent with the registered entity's Facility Ratings methodology that is used in the reliable planning and operation. SPP RE has identified inconsistences with Facility Ratings in operations and during monitoring engagements of registered entities.	FAC-008-3 R1, R2, R3
Event Response/ Recovery	SPP RE is expanding this risk element in response to increase control center outages. The purpose is to ensure plans, Facilities and personnel are prepared to perform through the training of personnel and testing of facilities.	EOP-008-1 R4

Regional Compliance Monitoring Plan

This section includes regional risk-based CMEP activities. The following is an overview of the year's currently known IRA, audit, spot check, periodic data submittals, and self-certifications.

The audit schedule is also located on the SPP RE's website here: 2017 Compliance Program.

SPP RE will perform an IRA for the registered entities to determine the monitoring activity and the individual monitoring scope. The assessment criteria will consist of a review of the registered entity's inherent risks and performance considerations as identified in the ERO Enterprise IRA Guide.

- **On-Site Audits** - SPP RE will continue to audit the Transmission Operator and Balancing Authority entities on a three-year cycle in 2017. In 2017, registered entities with high and medium BES Cyber Systems will have on-site CIP audits based upon a three-year cycle.
- **Off-Site Audits**- SPP RE will conduct Operation and Planning audits of the registered entities that were previously scheduled for an audit in 2017 based upon a six-year audit and based on the IRA. In addition, SPP RE will conduct off-site CIP audits for registered entities with low impact BES Cyber Systems after April 1, 2017. SPP RE may audit registered entities that have been registered within the last two years.
- **Spot-Checks** - Spot-Checks may be used in lieu of Off-Site audits for registered entities that have been identified as lower risk through the entity's IRA. There are no mandatory Spot Checks listed in the 2017 ERO Enterprise CMEP IP. However, SPP RE may initiate a Spot Check at any time to verify or confirm Self Certifications, Self-Reports, Periodic Data Submittals, Areas of Concerns identified in previous monitoring engagements or in response to operating problems or system events.
- **Self-Certification** - SPP RE will continue to require SPP RE registered entities to perform a Self-Certification to ensure that the registered entity is maintaining rigorous internal controls for ensuring compliance with the Reliability Standards. SPP RE may require Self-Certification in conjunction with other compliance monitoring methods. SPP RE has identified Self-Certification requirements based on the ERO Enterprise CMEP IP and Regional Assessment for the registered entities. Self-Certification will be conducted using webCDMS. Entities will receive additional notice and instructions before each quarterly or annual reporting window.
- **Periodic Data Submittal** - The 2017 ERO Enterprise CMEP IP does not identify Reliability Standards and Requirements that require periodic data submittals. SPP RE will require periodic data submittals for the specific Reliability Standards and Requirements that SPP RE, SPP RTO, MISO, and Lead Regional Entities collect for operational data on a monthly, quarterly, or annual basis.

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR01055	AES Shady Point, LLC (AESSP)	O&P	
NCR01061	Board Of Public Utilities (Kansas City KS) (BPU)		CIP
NCR11354	Canadian Hills Wind, LLC (CHW)		CIP
NCR11230	Caney River Wind Project, LLC (CRWP)		CIP
NCR06043	Central Valley Electric Cooperative, Inc. (CVEC)	O&P	
NCR10190	City Of Gardner (GARDNER)	O&P	
NCR10227	City Of Ottawa (OTTAWA)	O&P	CIP

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR01081	City Utilities Of Springfield, MO (SPRM)	O&P	
NCR01083	Cleco Corporation (CLECO)		CIP
NCR11250	Dogwood Power Management, LLC (DPM)		CIP
NCR06046	Farmers' Electric Cooperative, Inc. Of New Mexico (FARMCOOPNM)	O&P	
NCR11314	Flat Ridge 2 Wind Energy LLC (FRWEII)		CIP
NCR01101	Grand River Dam Authority (GRDA)	O&P	
NCR01103	Green Country Energy, LLC (GREENCOGO)	O&P	CIP
NCR01104	Green Country Operating Services, LLC (GREENCOGOP)	O&P	CIP
NCR01107	Kansas City Power & Light Company (KCPL)		CIP
NCR01109	Kansas Electric Power Cooperative, Inc. (KEPC)	O&P	
NCR11329	KODE Novus Wind I, LLC (KODE)		CIP
NCR01114	Lafayette Utilities System (LAFA)	O&P	
NCR01116	Louisiana Energy & Power Authority (LEPA)	O&P	
NCR06048	Lubbock Power And Light (LPLTX)	O&P	CIP
NCR01118	Midwest Energy, Inc. (MIDW)		CIP
NCR11236	NAES Corporation - Goodman Energy Center (NAESGEC)		CIP
NCR06054	North American Energy Services - Dogwood (NAESDOGW)		CIP
NCR01130	Oklahoma Gas And Electric Co. (OKGE)	O&P	
NCR11485	Oneta Power, LLC (ONETA)	O&P	
NCR11264	Post Rock Wind Power Project, LLC (PRWP)		CIP
NCR11410	Rita Blanca Electric Inc. (RBEC)	O&P	
NCR01142	Sikeston Board Of Municipal Utilities (SIKESTONMO)		CIP
NCR01143	Southwest Power Pool (SPP) - SERC		CIP
NCR01144	Southwestern Power Administration (SWPA)	O&P	
NCR11322	Spearville 3, LLC (SPEAR3)		CIP
NCR11323	Spinning Spur Wind, LLC (SPINSPUR)		CIP
NCR01155	The Empire District Electric Company (EDE)	O&P	CIP
NCR01357	USACE - Kansas City District (COEKS)	O&P	
NCR10226	Llano Estacado Wind, LP (LLANOEWIND) SPPRE LRE	O&P	CIP
NCR01019	Northern Iowa Wind Power 1, LLC (NIWP) SPPRE LRE	O&P	CIP

2017 Compliance Audit Plan			
Update NCR ID	Registered Entity/Coordinated Oversight LRE	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR01056	American Electric Power Service Corp. (AEPW) / RF LRE		CIP
NCR11570	Arbuckle Mountain Wind Farm LLC (AMWF) / RF LRE	O&P	CIP
NCR06040	Blue Canyon II Windpower LLC (BCWII) / RF LRE	O&P	CIP
NCR06041	Blue Canyon Windpower LLC (BCWI) / RF LRE	O&P	CIP

2017 Compliance Audit Plan			
Update NCR ID	Registered Entity/Coordinated Oversight LRE	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR03048	Blue Canyon Windpower V, LLC (BCWV) / RF LRE	O&P	CIP
NCR11201	Blue Canyon Windpower VI, LLC (BC6) / RF LRE	O&P	CIP
NCR11240	Cimarron Windpower II, LLC (CIMW) / Texas RE LRE	O&P	CIP
NCR10302	Cloud County Wind Farm, LLC, (CCWF) / RF LRE	O&P	CIP
NCR11241	Duke Energy Generation Services, Inc. (DEGS) / Texas RE LRE	O&P	CIP
NCR11257	Ironwood Windpower, LLC (IRONWOOD) / Texas LRE	O&P	CIP
NCR10400	ITC Great Plains, LLC (ITCGP) / RF LRE	O&P	CIP
NCR01145	Southwestern Public Service Co. (Xcel Energy) (SPS) / LRE MRO	O&P	CIP
NCR11577	Waverly Wind Farm LLC (Waverly) / RF LRE	O&P	CIP

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	Anticipated Date
SPP RE Newsletters	Monthly
SPP.org RE Webpage	Updated as needed
2017 Spring Compliance Workshop	March 28-29, 2017
2017 CIP Workshop	June 27-28, 2017
2017 Fall Compliance Workshop	October 24-25, 2017
Webinars and Training Videos	As developed
Event Analysis Lessons Learned	As developed

Appendix A7 - Texas Reliability Entity (Texas RE) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for the Texas RE as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

In 2016 Texas RE evaluated the risk based compliance monitoring implementation efforts and facilitated improvements in effectiveness and efficiency. Every registered entity selected for an engagement in 2017 will undergo an Inherent Risk Assessment (IRA) to focus efforts on reliability risks for the registered entity and focus Texas RE staff.

The approved Oversight Plan Development Framework does not require Texas RE to indicate which Compliance Monitoring Enforcement Program (CMEP) Tool (e.g., audit, spot check, self-certification) will be used in an engagement with Registered Entity candidates for 2017. Texas RE will follow the ROP requirements for notifying candidates once a CMEP Tool, as developed within the approved Oversight Plan Development Framework, is determined. The ROP requires that a Reliability Coordinator (RC), Balancing Authority (BA), or a Transmission Operator (TOP) will have an audit performed "at least once every three years". Those RCs, BAs, or TOPs meeting the "at least once every three year" designation will be listed in the Annual Audit Plan.

Texas RE will evaluate Electric Reliability Organization (ERO)-wide and Region specific Risk Elements and apply compliance monitoring processes for Standards and Requirements applicable to the risks selected. During the year, Texas RE may update the Implementation Plan. Updates can include, but are not limited to: changes to the compliance monitoring processes, changes to regional processes, updates resulting from a major event, FERC Order(s), or other matter(s) deemed appropriate by Texas RE or NERC. When updates occur, Texas RE will submit updates to the NERC, which will review and act on any proposed changes. NERC is responsible for updating the ERO Enterprise CMEP Implementation Plan (CMEP IP) to reflect any Texas RE changes. NERC will post the updated plan to the NERC website and issue compliance communications. Texas RE will evaluate Operations and Planning (O&P) Requirements and Critical Infrastructure Protection (CIP) Requirements concurrently during engagements rather than approaching Requirements relative to the risks separately.

As part of risk-based CMEP implementation, Texas RE enhanced an IRA tool. The IRA tool will undergo continuous improvements based on the IRA Guide, NERC oversight feedback, lessons learned, registered entity feedback, and the straightforward common sense approach by the Texas RE Risk group. During 2017 every registered entity engagement will start with an IRA and the results, which will be provided to the registered entity as an IRA Summary Report. Additionally, Texas RE appends the IRA Summary Report to the Non-Public engagement report for a registered entity. This action will provide a bookend to the engagement process so a registered entity, and any other participating party, can visualize key milestones in the engagement process.

Other Regional Key Initiatives and Activities

Texas RE will continue to engage in significant outreach associated with the CIP Reliability Standards throughout 2017. Texas RE will continue review of entity compliance with CIP-014 to better understand physical security risks posed to the Interconnection. Texas RE will continue its collaborative effort between NERC, the Regional Entities, and registered entities to identify and implement changes that enhance the effectiveness of the CMEP.

Regional Risk Assessment Process

The regional risk assessment process is a facet of Texas RE's efforts to adequately plan effective compliance monitoring in the Interconnection. The risk assessment process is used to determine compliance monitoring objectives, compliance monitoring scope, and an initial entity oversight plan. Sub-processes of the risk assessment process include: determining Risk Elements (Interconnection risks), conducting an IRA (entity-level Bulk Electric System (BES) risks), completing an Internal Controls Evaluation (ICE) (entity-level risk mitigation), and developing a Compliance Oversight Plan (COP) (monitoring scope for an entity or class of entities). The work-product of the BES risk assessment process is the determination of individual engagement type, individual engagement scope, and development of a comprehensive oversight plan for an entity or class of entities.

The process of evaluating BES risk fully satisfies the concerns of significance and compliance monitoring risk. The process work product is a BES risk-targeted scope. The risk assessment process may be used to perform both comprehensive and highly targeted compliance monitoring activities. There is no requirement to address all BES risks in a single, comprehensive checklist-style compliance monitoring activity. Monitoring of individual risks via multiple engagements may be used as an alternate and more effective approach. The premise of the reliability assessment process 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 BES. For entities that pose a limited reliability risk, minimum compliance monitoring activities may suffice. For entities that do pose a significant risk to reliability, it will be necessary for those entities to undergo effective compliance monitoring such as additional focused spot checks, a greater number of self-certifications, or broader and deeper audits of greater frequency.

To assist Texas RE in determining how much risk an entity poses to reliability, Texas RE uses dedicated staff to review risk within the Interconnection. The staff relies heavily on feedback from other groups within Texas RE such as Registration, Enforcement, Reliability Services, and Compliance to achieve an understanding of the risks encountered or emerging within the Interconnection. Additionally, Texas RE reviews externally, both locally and nationally, created reports and discussions focusing on reliability risks. The Risk Elements Guide provides basic guidance for determining risks that may require some level of compliance monitoring. Texas RE will utilize the Risk Elements Guide and enhance focus on risks within the Interconnection by involving local subject matter experts.

For example, the Texas RE Reliability Services department creates an annual assessment of reliability performance report.[19] Some aspects within the report correlate to the Risk Elements determined within the Risk Elements Guide but others are corollaries, such as "System inertia changes with resource mix " a localized issue due to the influx of renewable resources requiring localized focus. This localized focus could equate to a deeper review of the ERO IP Risk Elements such as, in this case, "Monitoring and Situational Awareness" and "Extreme Physical Events." Effects of the declining system inertia may be evident is system event responses both in terms of human responses and physical characteristics such as Primary Frequency Response. Primary Frequency Response has been identified as a risk to the Interconnection. There is a local working group, the "Performance, Disturbance, Compliance Working Group (PDCWG)" that is responsible for reviewing, analyzing, and evaluating the frequency control performance of the Interconnection. The PDCWG analyses generation loss events of 450 MW or greater and system event frequency deviations of +/- 0.1 Hz or greater. The BAL-001-TRE Standard defines the updated methodology for individual generator primary frequency response. As such, the Standard could be utilized in compliance monitoring efforts for 2017.

Establishing knowledge of a new entity is important in determining risk associated with a new entity. Texas RE carefully tracks new entities and will use registration input(s) as a way to help delineate the need to engage in compliance monitoring. The ERO IP states that monitoring of a particular registered entity may include more, fewer, or different Reliability Standards than those outlined in the ERO and Regional Entity CMEP IPs. Although the ERO IP and Regional IP identify NERC Standards and Requirements for consideration for focused compliance

[19] http://www.texasre.org/CPDL/2015%20Texas%20RE%20State%20of%20Reliability%20Report.pdf

monitoring, the ERO recognizes that the Framework and risk-based processes will develop a more comprehensive, but still focused, list of NERC Reliability Standards and Requirements specific to the risk a registered entity poses. Therefore, a particular area of focus under a risk element does not imply that: (1) the identified NERC Standard(s) fully addresses the particular risk associated with the risk element; (2) the NERC Standard(s) is only related to that specific risk element; or (3) all Requirements of a NERC Standard apply to that risk element equally.

Texas RE will utilize determined risks to facilitate engagements with Registered Entities in such a way that prioritizes the evaluation of compliance for the determined risks. Texas RE will apply the appropriate Risk Element or Risk Elements and other clearly articulated factors to the appropriate registered entity to maintain a focus on reliability. Each registered entity is subject to an evaluation of compliance for all Standards regardless of inclusion within the Areas of Focus described within the ERO IP. That fact allows, as indicated by the ERO IP, for a more in-depth review of additional requirements associated with risks beyond those shown within the ERO IP. As each entity represents a unique set of inherent risks to the Interconnection, Texas RE is committed to having each registered entity understand how the risks were developed for compliance monitoring engagements. Additional Risk Elements may be added as needed throughout the year.

Regional Risk Elements and Areas of Focus

The table below contains the Regional risk focus areas identified during the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of the registered entities COP.

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Critical Voltage Support	This risk element is based on existing and near-future system conditions, generation resources (i.e., type, availability, location, etc.), and voltage support capabilities in areas of the Interconnection in which voltage stability of the Bulk Electric System is a recognized risk. Historical events[20] have highlighted the risks associated with voltage control and stability. The need to actively monitor reactive resources within the system to ensure that voltage variations are minimized, preventing outages and damage to BES equipment, has been recognized as a risk. While voltage is generally a localized concern there has been a change in the ERCOT Interconnection that has facilitated the use of more dynamic and static reactive devices in more areas. Additionally, there are several load pockets where the management of reactive sources plays a significant role in ensuring reliability. The standards selected by Texas RE highlight Registered Entity responsibilities for providing, requesting, and ensuring that voltage support is available when needed.	TOP-004-2 R6; TOP-006-2 R1, R2; VAR-001-4 R1, R2, R5, R6; VAR-002-4 R1, R2, R5

[20] http://www.texasre.org/CPDL/2015%20Texas%20RE%20State%20of%20Reliability%20Report.pdf

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Facility Ratings	This risk element is focused on identifying potential gaps in the development and application of Facility Rating methodologies for Registered Entities. Through the use of CMEP activities, Texas RE has identified multiple instances in the ERCOT Interconnection in which Registered Entities have potential gaps and discrepancies in the development, application, and review of Facility Ratings. Failure of a Registered Entity to properly develop and apply Facility Ratings can result in potential high risk effects to the BPS. Those risks include improper identification and mitigation of System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs) and damage to BPS equipment and facilities. The standards selected are directly tied to developing and implementing Facility Ratings for a Registered Entity's BPS Facilities.	FAC-008-3 R1, R2, R3, R6, R7, R8; MOD-025-2 R1, R2, R3;
Operational Communication	This risk element highlights the various voice and data related communications required to operate within the ERCOT Interconnection. Due to the unique interactions between entities within this Interconnection, there are different process and responsibilities that Registered Entities face when providing the necessary voice and data related communications. As evidenced in some events, proper communication efforts and the results of the communication can affect the recovery response. This risk element highlights those processes to ensure that the necessary information is being requested and provided by Registered Entities within the ERCOT Interconnection. The wholesale electricity market in the Interconnection is regulated by the Public Utility Commission of Texas (PUCT). This market structure requires balanced market rules that help foster a stable electricity market. ERCOT market rules are developed by participants from all aspects of the electricity market in the ERCOT Interconnection. These market rules, known as ERCOT Protocols and Operating Guides, are enforced by the	COM-001-2 R10, R11; IRO-002-4 R4; IRO-010-2 R1, R3; IRO-017-1 R1, R2; PRC-001-1.1 (ii) R2; TOP-003-3 R1, R2, R3, R5; TOP-006-2 R1; VAR-002-4 R3, R4, R5

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	PUCT and have significant influence on the actions of Registered Entities. The ERCOT Protocols and Operating Guides include communication requirements and processes between Registered Entities and non-NERC Registered Entities that mirror or enhance NERC Reliability Standards. The processes defined within the ERCOT Protocols and Operating Guides provide very specific processes and responsibilities to Registered Entities and non-NERC Registered Entities within the Interconnection. This risk element highlights those processes to ensure that necessary data is being requested (e.g., outages of communication equipment or relays) and provided by Registered Entities within the Interconnection to support reliability and meet the NERC Reliability Standards. Communication supports reliability by providing awareness through effective monitoring. The standards selected by Texas RE highlight Registered Entity responsibilities regarding effective operational communication.	
SOL/IROL Management	SOL and IROL management have been historically recognized by Texas RE as a noteworthy issue[21] to track. Additionally, the industry determined that clarifications were needed regarding the definition of SOLs.[22] While IROL exceedances have trended downwards, there have been configuration changes within the Interconnection that have revealed new possible constraints. In the ERCOT Interconnection approximately 15% of tracked events have been loss of real-time monitoring or analysis tools. The new constraints coupled with possible loss of monitoring capability need thorough review to help ensure the reliability of the Interconnection. It is important to distinguish operating practices and strategies from the SOL itself. An SOL is based on the actual set of Facility Ratings, voltage limits, or Stability limits that are to be monitored for the pre- and post-Contingency state. Facility Rating methodology and	FAC-008-3 R1, R2, R3, R6; FAC-010-2.1 R1, R2, R3; FAC-010-3 R1, R2, R3; FAC-011-2 R1, R2, R3, R4; FAC-011-3 R1, R2, R3, R4; FAC-014-2 R5; IRO-006-TRE-1 R1, R2; PER-005-2 R4; TOP-002-4 R1, R2, R3, R4, R5, R6; TOP-004-2 R6

[21] http://www.texasre.org/CPDL/2014%20Texas%20RE%20Assessment%20of%20Reliability%20Performance.pdf

[22] http://www.nerc.com/pa/Stand/Prjct201403RvsnstoTOPandIROStndrds/2014_03_fifth_posting_white_paper_sol_exceedance_20150108_clean.pdf

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	implementation have been recognized as a risk that directly effects the establishment of SOLs. How an entity remains within these SOLs can vary depending on the planning strategies, communication practices with other entities, operating practices, System Operator training, and mechanisms employed by that entity. As indicated in other Risk Elements, the nature of the ERCOT Interconnection requires unique attention to the management of issues affecting the reliability of the Interconnection. The configuration changes have "retired" some IROLs and introduced new SOLs that impact the operation of the BES. The standards selected by Texas RE highlight the management of SOLs starting with the planning perspective. With the ERCOT Interconnection configuration continually undergoing significant change, it is critical to have adequate controls regarding all management aspects of SOLs in place to ensure the reliability of the Interconnection.	
SPS Management	Special Protection Systems (SPS) (Note: Remedial Action Scheme will effectively replace SPS on April 1, 2017) are used to provide an automatic response in an effort to prevent damage to equipment and loss of load based on very specific predetermined conditions. The SPS responses include changes in demand, generation, or system configuration in an effort to alleviate the abnormal condition. Failure to properly design and implement SPS could result in the SPS not being deployed correctly, which could result in system conditions exceeding device and facility limits. Failure to maintain SPS devices could result in a misoperation of the SPS, leading to the SPS failing to operate or operating prematurely. As demonstrated by a Texas RE report,[23] the arming of SPSs has indicated a slight trend upward whereas the number of SPSs has been trending downward. These trends are indicative of a possible risk associated with the management and utilization of the remaining SPSs within the Interconnection. The significant change in configuration which has, as indicated in the Texas RE report, reduced the number of SPSs within the Interconnection may be the catalyst for the increase in SPS arming. Increases in SPS arming may be indicative	IRO-005-3.1a R1; IRO-010-2 R1, R3; PRC-001-1.1(ii) R1, R6; PRC-005 R1, R2; PRC-015-1 R1 PRC-017-1 R1, R2

[23] http://www.texasre.org/CPDL/2014%20Texas%20RE%20Assessment%20of%20Reliability%20Performance.pdf

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	of possible changes in system configuration resulting in a difference in load flow. The configurations changes may be significantly different from the time an SPS was designed. While there has not been a misoperation of an SPS in the recent past, which may illustrate adequate controls regarding the maintenance and testing of SPS components beyond the Protection System components, the increase in arming of SPSs is a reliability concern. The standards selected by Texas RE highlight the planning, coordination, implementation, and monitoring of SPSs. The standards also highlight the maintenance and testing requirements for SPS devices.	
UFLS Management	Under frequency load shedding (UFLS) systems are used as an automatic response to deteriorating system conditions. As frequency drops the properly designed and implemented UFLS systems will automatically shed load in a coordinated effort to stabilize system conditions. These systems are rarely used but have high importance. Failure to properly design, implement, and maintain UFLS could result in the UFLS not being deployed correctly, which could result in system frequency continuing to degrade. Continued degradation could lead to frequency collapse. The ERCOT Interconnection is an island relying on UFLS activation as one of the last reliability related actions to thwart a complete collapse. The change in configuration, in terms of transmission and generation, of the ERCOT Interconnection could result in the utilization of UFLS. The standards selected by Texas RE highlight the planning, coordination, implementation, and monitoring of UFLS systems. The standards also highlight the maintenance and testing requirements for UFLS devices.	PRC-005 R1, R2; PRC-006-2 R1, R8, R9; PRC-008-0 R1, R2
UVLS Management	Under voltage load shedding (UVLS) systems are used as an automatic response to deteriorating voltage conditions. As voltage drops, locally or interconnection wide, the properly designed and implemented UVLS systems will automatically shed load to stabilize system conditions. These UVLS systems are used in system events affecting the Interconnection.	EOP-003-2 R2, R3, R4; PRC-005 R1, R2 PRC-010-0 R1; PRC-010-2 R1, R2, R3, R4, R5, R7; PRC-011-0 R1; PRC-022-1 R1

Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	Failure to properly design, implement, and maintain UVLS could result in the UVLS not being deployed correctly, which could result in system voltage continuing to degrade. Continued degradation could lead to voltage collapse. The standards selected by Texas RE highlight the planning, coordination, implementation, and monitoring of UVLS systems. The standards also highlight the maintenance and testing requirements for UVLS devices.	

Regional Compliance Monitoring Plan

Texas RE will monitor registered entities' compliance with Reliability Standards using the compliance monitoring processes described in Appendix 4C of the ROP. Texas RE will determine the type and frequency of application of the compliance monitoring tools appropriate for a particular Registered Entity based on the registered entity's specific risks to the reliability of the bulk power system. Each registered entity selected for an engagement in 2017 will undergo an IRA, or an IRA review, to focus efforts on reliability risks for the registered entity and focus Texas RE staff. The term "engagement" is considered by Texas RE as a Compliance Audit ("audit"), Spot Check, or Self-Certification which are forms of compliance monitoring processes described in Appendix 4C of the ROP. The IRA process will determine the type of compliance monitoring process that will be utilized.

The expectation of Texas RE is that the entities on the 2017 Candidate List will be subject to any one, or more, of the compliance monitoring processes. The overall engagement schedule (combination of the Annual Audit Plan and 2017 Candidate List) is dependent upon resource scheduling of registered entity staff and Texas RE CMEP staff. The target date for a completed IRA is no later than 105 days prior to a possible engagement to allow for the 90-day notification requirement for a Compliance Audit per the ROP. The notifications for any engagement, as defined in the ROP, shall be dependent upon the completion of an IRA. Texas RE and Registered Entities have been working well together to accommodate engagement schedule changes as needed. The Annual Audit Plan schedule, required for entities (i.e., TOPs, RCs, and BAs) is located on the Texas RE website here: [Annual Audit Plan] and is consistent with the ROP requirements.

Texas RE will perform IRAs on registered entities shown, and not shown, on the Annual Audit Plan schedule below. The approved Oversight Plan Development Framework does not require Texas RE to indicate which CMEP tool will be used in an engagement with registered entity candidates for 2017 at this point of the process. Texas RE will follow the ROP requirements for notifying candidates once a CMEP tool, as developed within the approved Oversight Plan Development Framework, is determined. The ROP requires that a RC, BA, or a TOP will have a Compliance Audit performed "at least once every three years". Those RCs, BAs, or TOPs meeting the "at least once every three years" criteria shall be listed in the Annual Audit Plan. Texas RE will utilize a risk-based compliance monitoring approach to engage with registered entities within the Texas RE footprint. Other registered entities that will be considered candidates for a compliance monitoring engagements in 2017 will be listed on the Texas RE website here [2017 Candidate List].

The format for the periodic data submittal schedule for 2017 is not expected to change significantly from the 2016 Data Submittal Schedule. If any changes are made to the 2017 Data Submittal Schedule, the schedule will be updated and affected entities would receive adequate notification of the change. The 2017 Data Submittal

Schedule reflects the efforts of the ERO to implement the Coordinated Oversight Program and is posted on the Texas RE website here.

2017 Compliance Audit Plan			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR04022	Bryan Texas Utilities	O&P	CIP
NCR04015	Brazos Electric Power Co Op, Inc.	O&P	CIP
NCR01186	Brazos Electric Power Cooperative, Inc.	O&P	CIP
NCR04032	City of College Station	O&P	CIP
NCR04109	Oncor Electric Delivery Company LLC	O&P	CIP
NCR04037	CPS Energy	O&P	CIP
NCR11076	Lone Star Transmission, LLC	O&P	CIP
NCR04056	Electric Reliability Council of Texas, Inc.	O&P	CIP
NCR04143	Texas-New Mexico Power Co	O&P	CIP

Compliance Outreach

Compliance Outreach Activities	
Outreach Activity	Anticipated Date
Spring Compliance Workshop	Spring 2017
Fall Compliance Workshop	Fall 2017
Talk with Texas RE	Projected Monthly (subject to change)
Texas *RE*view Newsletter	Projected Monthly

Appendix A8 - Western Electricity Coordinating Council (WECC) 2017 CMEP Implementation Plan

This Appendix contains the CMEP Implementation Plan (IP) for WECC as required by the North American Electric Reliability Corporation (NERC) Rules of Procedure (ROP).

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

In 2017, the Western Electricity Coordinating Council (WECC) will continue its practice, which began in 2015, to use the Compliance Monitoring Strategy (CMS) tool to aid in the development and tracking of WECC's Risk-Based Oversight Plans for monitoring activities, including Self-Certifications, Audits, Spot-Checks, Inherent Risk Assessments (IRA), and Internal Control Evaluations (ICE), as directed in the NERC ROP, Compliance Monitoring Enforcement Program (CMEP), and the annual WECC and NERC Implementation Plans (IP). In addition, WECC will leverage the information from IRAs, ICEs, lessons learned, Electric Reliability Organization (ERO) best practices, and other information to focus appropriate monitoring and enforcement efforts. WECC will continue to work with NERC and the other Regions in 2017 to improve consistency within the ERO for IRA and ICE processes.

Multi-Region Registered Entity (MRRE) Coordinated Oversight Program

WECC will continue to participate in the ERO Enterprise Coordinated Oversight program for Multi-Region Registered Entities. The program is designed to streamline risk assessment, compliance monitoring and enforcement, and event analysis activities for registered entities that have been approved to participate in the coordinated oversight program.

Regional Risk Assessment Process

WECC will continue its efforts to support and implement the ERO Risk-Based Compliance Oversight Framework described in the ERO CMEP IP. The 2017 ERO CMEP IP identifies Risk Elements and Areas of Focus, which provide the foundation for WECC's Regional Compliance Oversight Plan (COP).

The 2017 ERO CMEP IP does not constitute a comprehensive list of risks that may affect the bulk power system, so WECC considered regional and local risks along with the specific circumstances associated with individual registered entities within WECC's footprint when developing its Regional COP. WECC also considered the WECC 2016 State of the Interconnection report in our Regional Risk Assessment.

WECC will continue its engagement with NERC to ensure it supports and implements the ERO Enterprise initiatives. The risk assessment process enables WECC to focus its compliance monitoring activities on those Reliability Standards that pose the greatest risks to the reliable operation of the Bulk Electric System (BES) in the Western Interconnection.

Risk Factors and Inherent Risk Assessments

To identify inherent risks, WECC considered risk elements identified in the 2017 ERO CMEP IP. In addition, WECC will continue to consider factors on an individual basis for each registered entity, including its footprint, generation and transmission profile, interconnections, geographical locations, system events, compliance violation trends, Critical Infrastructure Protection (CIP) Bulk Cyber Systems (BCS) and impact, etc.

Regional Risk Elements and Areas of Focus

In an effort to maintain consistency, WECC adopted the Risk Elements and Areas of Focus identified in the 2017 ERO CMEP IP. In addition to that list, the table below contains three Areas of Focus identified by WECC during the Regional Risk Assessment process.

Regional Additions to 2016 ERO Areas of Focus		
Risk Element	**Justification**	**Areas of Focus**
Maintenance and Management of BPS Assets	WECC is expanding this risk element based on the number of transmission lines that pass through dense vegetation areas, and due to high growth vegetation in the Western Interconnection. WECC considers these three requirements critical for Maintenance and Management of BPS assets and for Situation Awareness and Monitoring for the BES.	FAC-003-4 R3 FAC-003-4 R4 FAC-003-4 R5

Regional Compliance Monitoring Plan

Inherent Risk Assessments

During 2017, WECC will use the ERO Risk-Based Compliance Oversight Framework described in the ERO CMEP IP to determine the scope and method for conducting compliance activities. WECC will focus on identifying, prioritizing, and addressing risks to the BES, thereby allowing WECC to focus resources where they are most needed. WECC will conduct IRAs and develop preliminary COPs for registered entities subject to three-year audit engagements listed in the 2017 audit schedule. At the conclusion of an audit for a given entity, WECC may revise the entity's COP. In doing so, WECC would consider factors such as footprint, generation and transmission profile, interconnections, geographical locations, system events, CIP BCS, impact and on-site audit observations. Any COP revisions will be shared with the registered entity.

Periodic Data Submittals

WECC will continue to monitor a number of Standards and Requirements that require data submittals on a monthly, quarterly, and/or annual basis. The list of Standards and Requirements is located on WECC's website.

Self-Certifications

WECC will perform guided self-certifications in 2017. The self-certification requests will focus on the risk based approach and scope will determined by WECC's quarterly CMS reviews, registered entity compliance history and/or results of IRA, COP and ICE. As part of the guided self-certification process, registered entities may be required to provide WECC with supporting evidence to substantiate determinations. The self-certification schedule is located on WECC's website.

Spot-Checks

WECC will use the ERO Risk-Based Compliance Oversight Framework described in the ERO CMEP IP to determine the scope and method for conducting compliance activities and may conduct random spot-checks as part of an entity's COP, to verify self-certifications, self-reports, periodic data submittals, mitigation plans, areas of concern and system events. WECC will notify registered entities of upcoming compliance engagements within the timeframes required by Appendix 4C to the NERC ROP.

Compliance Audits

The 2017 audit schedule is located on WECC's website.

2017 Compliance Audit Plan*			
NCR ID	Registered Entity	Type of Monitoring	
		Operations & Planning (O&P)	Critical Infrastructure Protection (CIP)
NCR05435	Turlock Irrigation District	O&P	CIP
NCR05223	Los Angeles Department of Water and Power	O&P	CIP
NCR05392	Silicon Valley Power	O&P	CIP
NCR05261	Nevada Power Company	O&P	CIP
NCR05390	Sierra Pacific Power Company	O&P	CIP
NCR05244	Modesto Irrigation District	O&P	CIP
NCR05333	Public Service Company of New Mexico	O&P	CIP
NCR11210	First Solar Electric, LLC	O&P	CIP
NCR11326	First Solar Electric - AVSR1, LLC	O&P	CIP
NCR11343	First Solar Electric - TPZ, LLC	O&P	CIP
NCR11358	First Solar Electric - ISECS, LLC	O&P	CIP
NCR11361	First Solar Electric - DSL, LLC	O&P	CIP
NCR11394	First Solar Electric - CVS, LLC	O&P	CIP
NCR11571	First Solar Electric-ISECSW, LLC	O&P	CIP
NCR11609	First Solar Electric-Red Hills, LLC	O&P	CIP
NCR11612	First Solar Electric-Stateline, LLC	O&P	CIP
NCR11673	First Solar Electric-Astoria I, LLC	O&P	CIP
NCR11677	First Solar Electric-Astoria II, LLC	O&P	CIP
NCR05382	Seattle City Light	O&P	CIP
NCR05325	Portland General Electric Company	O&P	CIP
NCR05342	Public Utility District No. 2 of Grant County, Washington	O&P	CIP
NCR05334	Public Utility District No. 1 of Clark County	O&P	CIP
NCR05182	Hetch Hetchy Water and Power	O&P	CIP
NCR05343	PUD No. 1 of Douglas County	O&P	CIP
NCR05461	Western Area Power Administration - Desert Southwest Region	O&P	CIP
NCR05434	Tucson Electric Power	O&P	CIP
NCR05537	USACE - Omaha District	O&P	
NCR05140	El Paso Electric Company	O&P	CIP
NCR05515	National Nuclear Security Administration - Los Alamos National Laboratory	O&P	

***WECC will use the approved ERO Risk-based Compliance Oversight Framework, as described in the ERO CMEP IP and will determine the schedule and scope of each audit based on the quarterly CMS reviews, compliance history and/or results of IRA, COP and ICE.**

Compliance Outreach

Compliance Oversight Workshop

The Compliance Oversight Workshop provides in-depth, in-person, detailed training and education through structured lecture and presentation, panels of experts, interactive dialogue in an open forum, with direct question and answer sessions and invaluable networking opportunities. Workshops cover the entire compliance sphere

focusing on attendees' and industry issues. These meetings provide direct access to the WECC registered entity Oversight management team, staff, and Subject-Matter Experts (SME). Participants may also attend telephonically or via video webinar.

Monthly Open Webinars

Since many of the questions the WECC Compliance Staff receives are very similar, WECC answers questions in an open forum for greater efficiency. WECC Compliance SMEs participate in this webinar and respond to questions. In fairness to everyone on the call, WECC does not address entity-specific questions and issues. Information on workshops and seminars (and others as they are finalized) along with the dates on which they are scheduled to occur will be posted on the WECC website.

Compliance Outreach Activities	
Outreach Activity	**Anticipated Date/Location**
WECC Open Webinar	Third Thursdays of most months
Compliance Oversight Workshop	March 27-31, 2017 Aurora, CO November 13-17, 2017 Portland, OR

Appendix B – Compliance Assessment Report

Compliance Assessment Process for Events and Disturbances

The ERO Enterprise encourages registered entities to perform an initial compliance assessment (CA) concurrent with the registered entity's event review and analysis. When completing a CA, the registered entity should follow these steps:

1. Refer to the causes and contributing factors of the event as determined by the registered entity's events analysis process.
2. Identify all applicable NERC Reliability Standards and Requirements that may have been implicated by the causes and contributing factors of the event.
3. After reviewing the facts and circumstances of the event, develop conclusions that are relevant to step 2 above as they apply to the applicable NERC Reliability Standards and Requirements.
4. Self-report any findings of noncompliance to the RE per the CMEP procedures.
5. Provide a copy of the CA report to the RE compliance organization. The CA should be accompanied by the separate Event Analysis Report, Brief Report, or similar document that provides sufficient information for the RE to understand the event.

Sample Compliance Assessment Report Template			
Event Cause or Contributing Factor	**Applicable Reliability Standards and Requirements**	**Details of CA Efforts**	**Findings**
Cause–Example 1	AAA-000-0 R 1	1. Identify the process used to assess compliance with this Requirement. 2. Identify any evidence that demonstrates compliance 3. Identify any evidence that suggests noncompliance	Finding conclusion
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. "XYZ Interface All Lines In Stability Guide" (document provided)	No findings of noncompliance