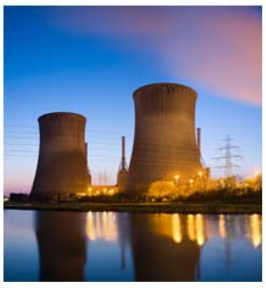
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2018 ERO Enterprise Compliance Monitoring and Enforcement Implementation Plan

Version 2.1

May 2018

RELIABILITY | ACCOUNTABILITY

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

Table of Contents

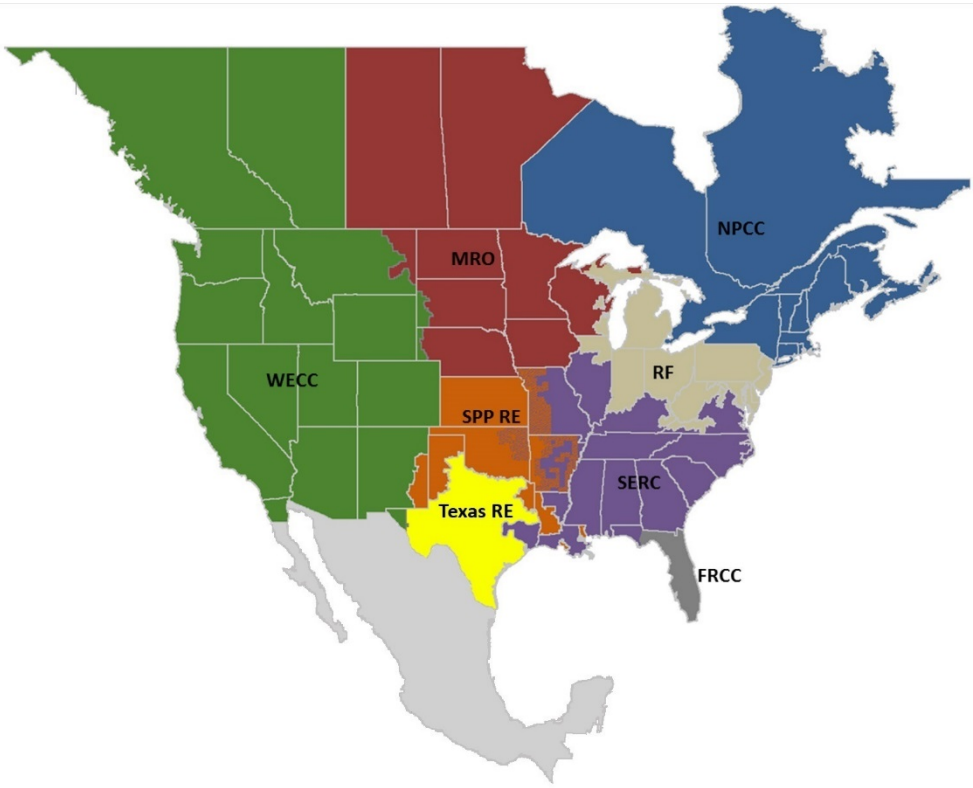
Revision History

Version	Date	Revision Detail
Version 1.0	September 08, 2017	• Release of the 2018 ERO CMEP Implementation Plan (IP). The ERO CMEP IP is the NERC portion only of the CMEP IP.
Version 2.0	November 21, 2017	• Updated with the eight Regional Entities' 2018 CMEP IPs in Appendices A1 – A8. • Included information on the 2018 ERO Enterprise Periodic Data Submittals Schedule.
Version 2.1	May 2, 2018	• Made significant updates to SPP RE Regional Appendix to reflect NERC's petition filed with FERC requesting to terminate the Regional Delegation Agreement between NERC and SPP. Updates include guidance from SPP RE on 2018 compliance monitoring activities under the Regional Compliance Monitoring Plan. • Updated MRO Regional Appendix to remove Guided Self-Certifications for MOD-008-1, MOD-025-2, and FAC-003-4. In addition, the MRO Security Conference is now planned for Fall 2018. • Updated RF Regional Appendix to remove references for tentatively scheduled Guided Self-Certifications.

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 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 Organization (ERO) Enterprise[1] Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) is the annual operating plan used by the ERO Enterprise in performing CMEP responsibilities and duties. The ERO Enterprise executes CMEP activities in accordance with the NERC Rules of Procedure (ROP) (including Appendix 4C), their respective Regional Delegation Agreements, and other agreements with regulatory authorities in Canada and Mexico.

The ROP requires NERC to provide an IP to the Regional Entities (REs) on or about September 1 of the preceding year.[2] 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 Regional Compliance Monitoring 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 to NERC and the 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 monitoring oversight of registered entities.

NERC is responsible for collecting and reviewing the RE IPs to help ensure REs provide appropriate and consistent information on 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.[3]

During the implementation year, NERC or an RE may update their portions of the IP. Updates may include, but are not limited to, the following: 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 an announcement.

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

[1] The ERO Enterprise is comprised of NERC and the eight Regional Entities, which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the EROs' statutory obligations to assure the reliability of the North American BPS.
[2] NERC ROP, Section 403 (Required Attributes of RE Compliance Monitoring and Enforcement Programs).
[3] ERO Enterprise Annual CMEP Reports available at http://www.nerc.com/pa/comp/Pages/AnnualReports.aspx

Significant CMEP Activities

The following ongoing activities impact the ERO Enterprise's CMEP implementation.

Program Alignment

Greater alignment across the ERO Enterprise can help maintain focus on the most significant risks to reliability through the use of aligned practices in the monitoring and enforcement of compliance with the Reliability Standards. The Program Alignment process is an opportunity to improve alignment throughout the ERO Enterprise by identifying approaches to ensure consistency and leverage ongoing efforts across the ERO Enterprise. The NERC Compliance and Certification Committee (CCC) also has a role to identify potential misalignments and frame issues for the ERO Enterprise to consider when planning its program alignment activities. In Q2 2017, these activities included developing processes for issue classification and tracking; identifying roles and responsibilities of NERC, the REs, and industry stakeholders such as the CCC; and continuing to consolidate various information sources from across the ERO Enterprise. These issues stem from stakeholder reporting, survey responses and regional input as well as areas identified through NERC's oversight activities. The CCC Consistency Working Group will support the ERO Enterprise in executing certain components of the Program Alignment.

The Program Alignment consists of the following:

- **Track**: Identify and capture issues
- **Triage**: Classify, analyze, and prioritize
- **Transparency**: Post and report

The overall elements of success of the program are capturing and centralizing all reported issues, encouraging industry participation to help define the issues with real examples, responding in a timely manner, and providing the appropriate level of transparency to industry. The ERO Enterprise plans to implement this program through documented processes owned and facilitated by NERC.

Compliance Guidance

A key factor in the success of compliance monitoring and enforcement of mandatory Reliability Standards rests on a common understanding among industry and ERO Enterprise CMEP staff of how compliance can be achieved and demonstrated. For many Reliability Standards, this is straightforward. For others, a variety of approaches may achieve the same objective. The Compliance Guidance process provides such a mechanism through the ERO Enterprise endorsement of Implementation Guidance and the development of CMEP Practice Guides.

Implementation Guidance is developed by industry and vetted through prequalified organizations. For an organization to become prequalified, a member of that organization must submit an application to the CCC. Vetted examples can then be submitted to the ERO Enterprise for endorsement, and the example would be given deference by the ERO Enterprise during CMEP activities with consideration of facts and circumstances if endorsed. Implementation Guidance would not prescribe the only approach to implementing a Reliability Standard, and registered entities would be allowed to choose alternative approaches that better fit their situation. Draft Implementation Guidance will be posted on NERC's website on the Compliance Guidance page[4] while it is being considered for ERO Enterprise endorsement. Once the Implementation Guidance is endorsed, it will be moved to the ERO Enterprise-Endorsed Implementation Guidance section. Draft Implementation Guidance that does not receive ERO Enterprise endorsement will be removed, and the document in the Non-Endorsed Implementation Guidance section will be updated with the rational.

[4] Compliance Guidance available at http://www.nerc.com/pa/comp/guidance/Pages/default.aspx

CMEP Practice Guides are developed by the ERO Enterprise to reflect the independent, objective, professional judgment of ERO Enterprise CMEP staff, and at times may be initiated following policy discussions with industry stakeholders. Following development, the CMEP Practice Guides are posted for transparency on the NERC website.

Since the inception of the Compliance Guidance process, the ERO Enterprise has reviewed over 30 submitted Implementation Guidance documents for endorsement and developed two CMEP Practice Guides. Throughout 2018, the ERO Enterprise will continue to review and act on Implementation Guidance documents submitted by industry as well as to evaluate the need for (and develop, where appropriate) CMEP Practice Guides.

Critical Infrastructure Protection (CIP) Reliability Standards Focused on Remote Access Security

NERC worked with the REs to conduct a comprehensive study that identified the strength of the CIP Version 5 remote access controls, the risks posed by remote-access-related threats and vulnerabilities, and appropriate mitigating controls consistent with FERC's directive in Order No. 822. The conclusions from the study were filed with FERC on June 30, 2017. Based on the findings of the Report Access Study, the ERO Enterprise will continue to focus on remote access and network security controls for compliance monitoring activities in 2018.

Physical Security NERC Reliability Standard CIP-014-2

One of the main continuing focus areas for physical security is to understand the activities of stakeholders that have developed security plans to mitigate risks of specific threats. The ERO Enterprise assessed, through CMEP activities, whether high-impact Control Centers are sufficiently protected by actions undertaken pursuant to the Reliability Standard, the quality of planned or implemented physical security controls, and the timelines used for implementing the security and resiliency measures.

Supply Chain Risk Management NERC Reliability Standard CIP-013-1

To effectively address risks to reliability from supply chain vulnerabilities, the NERC Board of Trustees (BoT) adopted a Resolution for Cyber Security – Supply Chain Risk Management Standards[5] that requested that NERC management promptly commence appropriate preparations for implementation of the Supply Chain Standards and regularly report to the BoT on such activities. The BoT requested that (i) NERC management, in collaboration with the appropriate NERC technical committees, industry representatives and appropriate experts, including representatives of industry vendors, further study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified, and (ii) NERC management provide an interim report to the Board related to the foregoing by no later than approximately 12 months after the adoption of these resolutions and a follow-up final report to the Board no later than approximately 18 months after the adoption of these resolutions.

[5] Resolution available at BoT Meeting August 2017 Agenda Item 9.a: Cyber Security – Supply Chain Risk Management

Risk-Based Approach to Compliance Monitoring and Enforcement

Compliance monitoring and enforcement must be "right-sized" based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of noncompliance. A risk-based approach is necessary for a proper allocation of resources and to encourage registered entities to enhance internal controls, including those focused on the self-identification of noncompliance.

The ERO Enterprise Risk-Based Compliance Monitoring and Enforcement focuses on identifying, prioritizing, and addressing risks to the BPS to focus resources where they are most needed and likely to be the most effective.

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, enabling each RE 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 through use of the Framework. This process is described in more detail in the ERO Enterprise's Risk-Based CMEP.[6]

During 2018 and beyond, the ERO Enterprise will continue deploying processes and tools to support risk-based compliance monitoring. NERC and the REs are committed to implementing risk-based compliance monitoring, and plan to continue communications, training, and outreach throughout 2018.

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 interdependent.

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 this document.

The REs determine 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.[7] An IRA considers factors like 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 2018 ERO Enterprise CMEP IP. Rather, the IRA considers multiple factors to focus oversight to entity-specific risks and results in the identification of the Reliability Standards and Requirements that should be monitored.

When developing 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

[6] Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program
[7] ERO Enterprise Guide for Compliance Monitoring

through the processes outlined in the ERO Enterprise Guide for Internal Controls.[8] As a result of the Internal Control Evaluation (ICE) and other considerations, the REs may further refine the focus of compliance monitoring activities for a given entity and may, for example, limit the depth or focus of testing for a given area.[9]

Coordinated Oversight of Multi-Region Registered Entities

The ERO Enterprise offers coordinated oversight for multi-Region registered entities (MRREs)[10] to streamline the compliance monitoring and enforcement activities for the registered entities that use, own, or operate assets in areas covering more than one RE territory.

REs will coordinate their oversight responsibilities for MRREs in coordinated oversight by designating one or more Lead RE (LRE) to each MRRE or a group of MRREs. 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. Coordinated oversight for MRREs is flexible and voluntary for MRREs.

Periodic Data Submittals

Registered entities provide the required information to the CEA, either NERC or the REs, in accordance with the NERC ROP and CMEP. For the 2018 implementation year, NERC and the REs developed a consolidated schedule for the ERO Enterprise.

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 Reliability 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 the CA Process

The registered entity Compliance Assessments constitute a major element of the overall 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 encouraged to share the CA with the RE for all Category 2-and-above events and any Category 1 and uncategorized events that were significant and could help to increase awareness of reliability risks. 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.

[8] ERO Enterprise Guide for Internal Controls

[9] 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.

[10] Coordinated Oversight of MRRE Program Development and Implementation, available at MRRE Coordinated Oversight Program

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 Reliability Standards and, as appropriate, self-reporting.

Regional Entity Responsibilities in the CA Process

REs play a key role in the CA Process. Their familiarity and direct contact with the registered entities position the RE to affect the CA Process Outcome in a significant and positive manner. REs should take measures to promote the development and submittal of Compliance Assessments for Category 2-and-above events by the registered entities, working closely with the registered entities to ensure that the Compliance Assessments are complete, timely, and accurate, and that they create a clear picture of all significant elements of the event. 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 should 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 understand the event. The subsequent RCE is therefore based on a complete understanding of the event from the directly involved registered entities and reflects any required compliance follow-up.

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. Events described as “Category 2 and above” typically constitute significant challenges to BES reliability and may stem from violations of or gaps in the Reliability Standards. Consequently, prompt completion of the RE RCE is critical to ensure any deficiencies are quickly identified and corrected. 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 encourages 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. Valued behaviors that may mitigate penalty amounts include registered entity cooperation, accountability (including acceptance of responsibility for violations), a 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 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[11] continues to allow the ERO Enterprise to dispose efficiently of noncompliance posing a minimal risk to the reliability of the BPS, and to enhance its focus on noncompliance posing a greater risk to BPS reliability. In June 2017, NERC and FERC completed their second 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 but three samples and observed significant improvement in the clear identification of root cause. Risk assessment of noncompliance and identification of root cause are two areas of focus for the ERO Enterprise throughout 2017 and into 2018.

Mitigation Process Review and Examination of Repeat Noncompliance

Effective mitigation of noncompliance can reduce the immediate risk to reliability and reduce the likelihood that the noncompliance will recur and create additional risks. The ERO Enterprise is analyzing repeat noncompliance to gain a better understanding of common factors that may contribute to registered entities engaging in recurring conduct that results in repeat noncompliance. In some cases, less-than-adequate design or execution of mitigation activities may create a situation that allows noncompliance to repeat itself, sometimes with expanded scope and increased risk to reliability.

[11] Compliance Exception Overview

In July 2017, NERC began a Mitigation Process Review to evaluate the effectiveness of each RE's mitigation review practices and to ensure compliance with the NERC CMEP. The purpose of this effort was to ensure the REs are fostering reliable practices by registered entities to identify the root cause of noncompliance and develop robust mitigation activities. Comprehensive mitigation activities include not only ending the instant noncompliance but also implementing controls that can prevent and detect subsequent noncompliance. If appropriate, NERC will recommend enhancements to the REs' mitigation review programs based on the results of this review.

2018 ERO Enterprise Risk Elements

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 that 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 2017 risk elements to determine applicability for 2018.[12] Although the IP identifies NERC Standards and Requirements to be considered 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 Reliability Standard(s) fully addresses the particular risk associated with the risk element, 2) that the identified Reliability Standard(s) is only related to that specific risk element, or 3) that all Requirements of a Reliability Standard apply

[12] Appendix B, ERO Enterprise Guide for Compliance Monitoring

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 Reliability Standards and Requirements.

Risk Element Results

The 2018 risk elements are included in Table 1 and remain unchanged from 2017. Table 1 also provides historical risk element information from 2016 and 2017. The eight risk elements below are not a comprehensive list of all risks to the reliability of the BPS. Reliability Standards, Requirements, and associated functions for each area of focus may be updated throughout the year to reflect new versions of the Reliability Standards that become effective.

NERC identified the risk elements listed below using the risk element development process,[13] which includes taking into account the risks noted in the Reliability Issues Steering Committee's (RISC) report.[14] Additionally, NERC staff also collects data, reports, and publications that identify reliability risks such as the State of Reliability Report,[15] the Long-Term Reliability Assessment, publications from the RISC, special assessments, the ERO Enterprise Strategic Plan, and ERO Event Analysis Process insights.

Areas 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 do the areas of focus encompass 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 2018 have been identified along with the succeeding version of the Reliability Standard, or area focus, in each of the corresponding risk element tables: see Table 2 through Table 9.

Table 1: Critical Comparison of 2016, 2017, and 2018 Risk Elements

2016 Risk Elements	2017 Risk Elements	2018 Risk Elements
Critical Infrastructure Protection	Critical Infrastructure Protection	Critical Infrastructure Protection
Extreme Physical Events	Extreme Physical Events	Extreme Physical Events
Maintenance and Management of BPS Assets	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 Failures	Protection System Failures	Protection System Failures
Event Response/Recovery	Event Response/Recovery	Event Response/Recovery
Planning and System Analysis	Planning and System Analysis	Planning and System Analysis
Human Performance	Human Performance	Human Performance

[13] ERO Enterprise Guide for Compliance Monitoring; October 2016
[14] ERO Reliability Risk Priorities; November 2016
[15] NERC *State of Reliability 2016*

Critical Infrastructure Protection

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

While CIP is identified as a separate risk element, the CIP Reliability Standards themselves are linked to other risk elements identified in this document. The CIP Reliability 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 Reliability 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).

Unauthorized Access

Unauthorized access can lead to BES Cyber Systems (BCSs) being compromised and is a major risk to systems that are used to monitor and control the BPS. Based on the results of NERC's Remote Access Study, many systems used to operate the BES rely on remote access technologies. Remote access refers to the ability to access a system, application, or data from a remote location. Remote access can take one of two forms: 1) human- or user-initiated remote access, referred to as Interactive Remote Access in NERC's CIP Reliability Standards; or 2) automated system-to-system access. Registered entities frequently use Interactive Remote Access technologies to enable remote users to operate, support, and maintain control systems networks and other BES Cyber Systems. Among other things, providing for remote access enables users to efficiently access Cyber Assets to troubleshoot application software issues and repair data and modeling problems that cause application errors. These remote access technologies–while important for efficiently operating, supporting, and maintaining Cyber Assets, including those for control systems–could open up attack vectors. If not properly secured, remote access could result in unauthorized access to a registered entity's network and control systems with potentially serious consequences. For instance, an attacker could breach an environment via remote access by deliberately compromising security controls to obtain privileged access to critical systems. Although registered entities generally do not rely on Internet-facing systems to operate and monitor the BES, malicious actors have demonstrated capabilities to infiltrate systems that are not Internet-facing, such as systems designed to run autonomously with minimal human interaction and other mission-critical applications that are used to perform supervisory control that, if misused, could result in serious reliability issues. Additionally, a compromised device that is allowed to remotely access a Cyber Asset can serve as a gateway for cyber-criminals to attack networks.

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 that 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**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
CIP-002-5.1: Cyber Security - BES Cyber System Categorization	R1, R2	n/a	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-005-5: Cyber Security - Electronic Security Perimeter(s)	R1, R2	n/a	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-006-6: Cyber Security - Physical Security of BES Cyber Systems	R1, R2, R3	n/a	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
CIP-007-6: Cyber Security - System Security Management	R1, R2, R3, R5	n/a	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

Extreme Physical Events

Extreme physical events can include extreme natural events or physical security vulnerabilities that cause extensive damage to equipment and facilities. As concluded in the RISC report, widespread damage to certain types of BPS infrastructure can extend outages due to unavailability of nearby replacement equipment or specialized capabilities. The potential consequences of such events are high enough to warrant increased focus to properly address the risk to reliability.

Extreme Natural Events

The RISC report identifies severe weather or other natural events—e.g., hurricanes, tornadoes, prolonged extreme temperatures, Geomagnetic Disturbances (GMDs), floods, earthquakes, etc.—as one of the leading causes of outages. Severe weather can cause BPS equipment damage, fuel limitations, and disruptions of voice and data communications, which can cause loss of load for an extended period. 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 comprises physical security vulnerabilities. As stated in the RISC report, intentional damage, destruction, or disruption to facilities can cause localized-to-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/Future Enforcement Date *(if applicable)*	Entities for Attention
EOP-010-1: Geomagnetic Disturbance Operations	R1, R3	n/a	Reliability Coordinator Transmission Operator
CIP-014-2: Physical Security	R1, R2, R3, R4, R5, R6	n/a	Transmission Owner
TPL-007-1: Transmission System Planned Performance for Geomagnetic Disturbance Events	R1	n/a	Planning Coordinator Transmission Planner

Maintenance and Management of BPS Assets

As the BPS ages, less-than-adequate 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. The failure to properly commission, operate, maintain, prudently replace, and upgrade BPS assets generally could result in more frequent and wider-spread outages, and these could be initiated or exacerbated by equipment failures.
Another risk, highlighted by NERC's 2010 Facility Ratings Alert to industry, involved the misalignment between the design and actual construction of BPS facilities. NERC's Modeling Working Group also recommended implementation of data change management processes that include Reliability Requirements for Generator Owners and Transmission Owners to notify Transmission Planners, Transmission Operators, Reliability Coordinators, Planning Coordinators, et al. whenever there are changes made to the system that must be reflected in planning, operational, and real-time models.[16]

Additionally, compliance data analysis shows that PRC-005 has a high number of reported noncompliance and serious or moderate risk filings. This indicates a risk to reliability from entities lacking robust maintenance programs.

Transmission outages related to inconsistent vegetation management pose an ongoing reliability risk to the BPS. The 2016 Vegetation Report published by NERC shows a slight increase in grow-in-vegetation-related outages.[17] As a result, NERC has included vegetation management as an area of focus again in 2018. 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.

[16] Discrepancies Between RTCA and Planning Models
[17] Vegetation-Related Transmission Outages

Areas of Focus

Table 4: Maintenance and Management of BPS Assets			
Standard	**Requirements**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
FAC-008-3: Facility Ratings	R6	n/a	Generator Owner Transmission Owner
FAC-003-4: Transmission Vegetation Management	R1, R2, R6, R7	n/a	Generator Owner Transmission Owner
PRC-005-6: Protection System, Automatic Reclosing, and Sudden Pressure Relaying	R3, R4, R5	n/a	Distribution Provider Generator Owner Transmission Owner

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 of 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 of such a failure is the August 14, 2003 Blackout. NERC analyzed data and identified that outages of tools and monitoring systems are fairly common occurrences. Increased focus on this discovery has led to publishing reliability guidelines, NERC advisories, and lessons learned to help mitigate the impact of these occurrences.

Areas of Focus

Table 5: Monitoring and Situational Awareness			
Standard	**Requirements**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
IRO-002-5: Reliability Coordination – Monitoring and Analysis	R5, R6	n/a	Reliability Coordinator
IRO-008-2: Reliability Coordinator Operational Analyses and	R4	n/a	Reliability Coordinator

Table 5: Monitoring and Situational Awareness			
Standard	**Requirements**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
Real-time Assessments			
IRO-018-1(i): Reliability Coordinator Operational Analyses and Real-time Assessments	R1, R2, R3	04/01/2018	Reliability Coordinator
PRC-001-1.1(ii): System Protection Coordination	R6	n/a	Balancing Authority Transmission Operator
TOP-001-3: Transmission Operations	R10, R11, R13	06/30/2018	Balancing Authority Transmission Operator
TOP-001-4*: Transmission Operations	R10, R11, R13	07/1/2018	Balancing Authority Transmission Operator
**Replaces TOP-001-3 as per dates noted*			
TOP-010-1(i): Real-time Reliability Monitoring and Analysis Capabilities	R1, R2, R3, R4	04/01/2018	Balancing Authority Transmission Operator

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. Such coordination errors occurred in the Arizona-Southern California Outages (see recommendation 19),[18] the August 14, 2003 Blackout (see recommendation 21),[19] and the Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015 (see recommendation 2).[20]

The RISC report indicates the speed at which new technology resources are being integrated in some areas impacts the ability of planners to study scenarios and update system models. In addition, the "Resource Interruption Disturbance Report"[21] highlights potential risks to the BPS reliability due to erroneous tripping of inverter-based resources during faults on the power system regardless of their location or configuration.

Furthermore, 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. Generating plant protection schemes and their settings should be coordinated with

[18] See Arizona-Southern California Outages on September 8, 2011
[19] See Final Report on the August 14, 2003 Blackout
[20] See Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015
[21] See 1,200 MW Fault Induced Solar Photovoltaic Resource Interruption Disturbance Report, Southern California 8/16/2016 Event, June 2017

transmission protection, control systems, and system conditions to minimize unnecessary trips of generation during system disturbances.[22]

Linkage between Misoperations and Transmission-Related Qualified Events [23]

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.[24] 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. Relay ground function misoperations were reduced to six events in 2015. It was further reduced to only one event in 2016. The focus on the relay ground function has been attended by a reduction in its involvement in qualified events. It is not clear if any statistical basis will be able to confirm that its role in relay misoperations has been similarly decreasing.

Areas of Focus

Table 6: Protection System Failures

Standard	Requirements	Inactive/Future Enforcement Date *(if applicable)*	Entities for Attention
PRC-001-1.1(ii): System Protection Coordination	R3, R4, R5	n/a	Generator Operator Transmission Operator
PRC-004-5(i): Protection System Misoperation Identification and Correction	R1, R5	n/a	Generator Owner Transmission Owner
PRC-024-2: Generator Frequency and Voltage Protective Relay Settings	R1, R2	n/a	Generator Owner

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 report identified that 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.

An additional risk to event response and recovery is the unavailability of generators. Extreme weather conditions (e.g., 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 while at the same time curtailing power generation capability and fuel availability. 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.

[22] Considerations for Power Plant and Transmission System Protection Coordination, July 2015
[23] See NERC *2017 State of Reliability* report (p.175)
[24] See DRAFT ERO Event Analysis Process Version 3.1

The effects of extreme weather (e.g., 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 to reliability (e.g., simultaneous forced outages, de-ratings, and failures to start of multiple generating units). When extreme weather is present over a large geographic area, the combined impact on the fuel supply, power plant operations, generation unavailability, and heightened electricity demand can lead to severe reliability issues.

These extreme conditions occur beyond the extent of planned stress conditions, anticipated severe operation conditions, or fuel supply availability expectations. Further, such events may outstrip forecasts of residential and commercial electricity demand. These forecasts serve as the baseline for planning the BPS and for operators determining the amount of electric generation needed during critical periods. When the combination of some or all of the effects of extreme weather occurs, operators may be forced to manage severe unanticipated scenarios or generation shortages, prompting curtailments or load shed in local areas to maintain BES reliability in the overall grid.

Areas of Focus

Table 7: Event Response / Recovery

Standard	Requirements	Inactive/Future Enforcement Dates *(if applicable)*	Entities for Attention
CIP-008-5: Cyber Security - Incident Reporting and Response Planning	R2, R3	n/a	Reliability Coordinator Transmission Operator Balancing Authority Generator Operator Transmission Owner Generation Owner
CIP-009-6: Cyber Security – Recovery Plans for BES Cyber Systems	R2, R3	n/a	Reliability Coordinator Transmission Operator Balancing Authority Generator Operator Transmission Owner Generation Owner
EOP-011-1: Emergency Operations	R1, R2	n/a	Balancing Authority Transmission Operator
TOP-001-3: Transmission Operations	R12, R14	06/30/2018	Reliability Coordinator Transmission Operator
TOP-001-4*: Transmission Operations	R12, R14	07/01/2018	Reliability Coordinator Transmission Operator
IRO-001-4: Reliability Coordination – Responsibilities and Authorities	R1	n/a	Reliability Coordinator Transmission Operator
**Replaces TOP-001-3 per dates noted*			

Planning and System Analysis

Planning and system analyses are performed for the integration and management of system assets. This includes the analyses of other emerging system issues and trends (e.g., significant changes to the use of demand-side management programs, the integration of variable energy resources, changes in load characteristics, increasing

dependence on natural gas-fired generation, increasing uncertainty in nuclear generation retirements, and essential reliability services). NERC's annual *Long-Term Reliability Assessment*[25] forms the basis of NERC's assessment of emerging reliability issues.

There continues to be an unprecedented capacity shift that has promoted new generating plants powered by natural gas, new wind and solar units, generating plant deactivations, and market impacts introduced by demand resources and energy efficiency programs. Not only does natural-gas-fired generation capacity exceed coal, but is also the majority of generation seeking capacity interconnection rights. As a result of this abundance of gas-fired generation capacity, winter criteria analyses should include testing gas pipeline contingencies (e.g., a failure of a gas pipeline or a compressor station). The contingency set should be reviewed and validated periodically to ensure accuracy. These operational risks are a growing concern and were recently highlighted in a NERC Short-Term Special Assessment.[26]

The change in resource mix (retirement of conventional generation with projected addition of natural gas and renewable resources) can alter power flows and can reduce essential reliability services for voltage, frequency, and ramping support. Due to the change in resource mix, reserve margins may continue to tighten over the next five years, approaching requisite reference margin levels. Operating at or near the reference margin level, in addition to intermittent availability of wind and solar resources, creates a new operating reality for entities where emergency operating procedures are more likely.

The increase of asynchronous resources has the potential to significantly affect the system characteristics of frequency response. With the increasing use of asynchronous generation and other electronically-coupled resources, the level of synchronous inertial response is reduced. This leads to a need to consider both the amounts of synchronous inertia and the available amounts of frequency response based on expected conditions.[27] Frequency response must be carefully monitored to ensure that the inclusion of those new resources do not expose the system to unacceptable frequency excursion.

Maintaining adequate levels of system voltage is critical to BPS reliability and is achieved by resources' capability to absorb or produce reactive power. In order to maintain reliable operation of the Interconnection, generators should provide reactive support and voltage control within the generator facility capabilities. Voltage issues are local and require support from nearby generators or devices such as static or dynamic reactive resources. Adequately modeled operations and planning cases become increasingly critical as a changing resource mix, deployment of new technologies, etc., affect the risk to BPS reliability.

Areas of Focus

Table 8: Planning and System Analysis

Standard	Requirements	Inactive/Future Enforcement Date *(if applicable)*	Entities for Attention
BAL-003-1.1: Frequency Response and Frequency Bias Setting	R1	n/a	Balancing Authority
TOP-002-4: Operations Planning	R2, R4, R5	n/a	Balancing Authority

[25] 2016 Long-Term Reliability Assessment
[26] Short-Term Special Assessment; Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation; May 2016
[27] 2016 Long-Term Reliability Assessment

Table 8: Planning and System Analysis			
Standard	**Requirements**	**Inactive/Future Enforcement Date *(if applicable)***	**Entities for Attention**
TPL-001-4: Transmission System Planning Performance Requirements	R1, R2, R3, R4	n/a	Planning Coordinator Transmission Planner
FAC-014-2: Establish and Communicate System Operating Limits	R1, R5	n/a	Reliability Coordinator Transmission Operator
MOD-032-1: Data for Power System Modeling and Analysis	R2	n/a	Balancing Authority Generator Owner Resource Planner Transmission Owner Transmission Service Provider
MOD-025-2: Verification and Data Reporting of Generator Real and Reactive Power Capability and Synchronous Condenser Reactive Power Capability	R1, R2, R3	n/a	Generator Owner Transmission Owner that own synchronous condensers
MOD-026-1: Verification of Models and Data for Generator Excitation Control System or Plant Volt/Var Control Functions	R2	7/1/2018	Generator Owner
MOD-027-1: Verification of Models and Data for Turbine/Governor and Load Control or Active Power/Frequency Control Functions	R2	7/1/2018	Generator Owner
VAR-002-4: Generator Operation for Maintaining Network Voltage Schedules	R2	n/a	Generator Operator Generation Owner
VAR-001-4.1 Voltage and Reactive Control	R1, R2, R5	n/a	Transmission Operators

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.

NERC hosts an annual Human Performance conference to address these issues. The systematic investigation and evaluation of events in the bulk power system are uncovering many of the system's latent errors. Through the events analysis initiative and the use of Human Performance analysis and applications, the lessons learned and good industry practices are being applied to further improve the reliability of the BPS.[28]

Violation data indicates some registered entity personnel lack adequate cyber security training. This resulting lack of awareness and knowledge, coupled with recent activity with ransomware and other forms of malware, significantly increase the potential impact on the ability to respond and take actions to recover the BPS. Achieving a heightened awareness and preparation increases the ability to respond and recover from cyber attacks. This requires ensuring all appropriate staff are trained on the potential impacts and have advance planning for responding to and recovering from a cyber attack.

NERC's annual *State of Reliability*[29] forms the basis of NERC's measure of ongoing system performance to identify risks to reliability. One of the key findings of the report is that transmission outage rates caused by human error show a slight increase, but no increase in outage severity. The number of automatic (momentary and sustained) transmission outages from human error significantly reduced from 2014 to 2015. Year-end 2016 data demonstrates a return to 2014 levels. While no increase in outage severity was discovered, human error remains a major contributor to transmission outage severity and will remain an area of focus.

Areas of Focus

Table 9: Human Performance

Standard	Requirements	Inactive/Enforcement Date *(if applicable)*	Entities for Attention
COM-002-4: Operating Personnel Communications Protocols	R4, R5	n/a	Reliability Coordinator Transmission Operator Balancing Authority
PER-005-2: Operations Personnel Training	R3, R4, R6	n/a	Reliability Coordinator Transmission Operator Balancing Authority Generator Operator
CIP-004-6: Cyber Security - Personnel & Training	R2	n/a	Reliability Coordinator Transmission Operator Balancing Authority Generator Operator Transmission Owner Generation Owner

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

[28] NERC Human Performance site
[29] 2017 State of Reliability

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.);
- review and categorize potential RE-specific risks; and
- identify associated Reliability Standards and Requirements for IRAs, review of internal controls, 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 since RE risk elements should be viewed as incremental to the ERO risk elements.

Regional Compliance Monitoring Plan

Based on RE consideration and assessment of ERO Enterprise risk elements and Regional Risk Assessments, each RE will provide details on its regional compliance monitoring plan. The regional plans include a list of planned compliance monitoring activities for Compliance Audits, Spot Checks, Self-Certification, and Periodic Data Submittals. REs consider risk elements, both ERO-wide and Regional, entity-specific risks, and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with NERC Reliability Standards. These Regional compliance monitoring plans are included in Appendices A1 through A8 of this plan.

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' compliance 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.

NERC oversight and regular training will help ensure that all processes discussed herein are implemented in a consistent manner throughout the ERO Enterprise.

Appendix A1: Florida Reliability Coordinating Council (FRCC) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- FRCC has implemented a combined review process for entity noncompliance activities identified through any of the CMEP activities. The process will include Subject Matter Experts (SMEs) from FRCC Monitoring, Risk Assessment & Mitigation, and Enforcement. This approach provides a comprehensive process going into disposition determination. The enforcement disposition determination team will then provide feedback to Monitoring and Risk Assessment & Mitigation for future monitoring considerations and risk analysis of the entity.
- FRCC will continue to participate in coordinated oversight of MRREs. Currently, three FRCC-registered entities are participating in coordinated oversight. FRCC is an ARE for each.
- FRCC will continue to implement processes and approaches related to the updated IRA guidance in the ERO Enterprise Guide for Compliance Monitoring.
- FRCC will continue its CIP outreach as part of the activities identified in the Compliance Outreach section below.
- FRCC will continue to review internal controls during an entity monitoring engagement to understand an entity's systems for assessing, reporting, and improving their compliance program performance.

Regional Risk Assessment Process and Results

The FRCC has reviewed the eight ERO Enterprise Risk Elements and associated Areas of Focus and concurs with the specified NERC Reliability Standards and Requirements, with the following additions documented below in the Regional Risk Elements and Areas of Focus section.

FRCC will continue its annual process of receiving input from registered entity SMEs, Regional Entity Compliance Committee Forum (RECCF) members, for FRCC compliance staff consideration on areas they believe may contribute additional risk to the FRCC region. The RECCFs provided input in September of 2017 for consideration in FRCC's Regional Risk Assessment process in developing our 2018 FRCC CMEP IP.

FRCC considered the following local risk factors and identified additional NERC Reliability Standards and Requirements for monitoring as detailed below in the Regional Risk Elements and Areas of Focus section.

Number and Type of Registered Functions

As of September 1, 2017, FRCC has 42 registered entities. The registered functions are further defined below:

- Balancing Authority (BA)
- Distribution Provider (DP)
- Generator Operator (GOP)
- Generator Owner (GO)
- Planning Authority (PA)

- Resource Planner (RP)
- Reserve Sharing Group (RSG)
- Transmission Operator (TOP)
- Transmission Owner (TO)
- Transmission Planner (TP)
- Transmission Service Provider (TSP)

FRCC (Member Services Division) is registered as a Reliability Coordinator (RC) and Planning Coordinator (PC). The SERC RE 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 NERC Reliability Standards due to registered functions.

Geographic Location, Seasonal or 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 NERC 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 NERC 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 BPS transmission lines located in the FRCC Region, and therefore has not included additional NERC 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 NERC 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 NERC 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 NERC Reliability Standard for Automatic Underfrequency Load Shedding have been added.

Special Protection Schemes (SPSs)

The FRCC considers factors such as any major SPSs installed in the FRCC Region when considering additional NERC 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 NERC Reliability Standards for Automatic Underfrequency Load Shedding, Special Protection System Misoperations, and Special Protection System Maintenance and Testing have been added.

Regional Risk Elements and Areas of Focus

Table A1.1 contains the Regional risk elements, and expanded ERO risk elements, for focus during the 2018 calendar year based on the Regional Risk Assessment process. The table also contains areas of focus regarding identified risks that may be considered in the development of a registered entity's Compliance Oversight Plan (COP).

Table A1.1: Additional Areas of Focus for ERO Risk Elements

Expanded ERO Risk Element	Justification	Associated Standard 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 EOP-008-1 R7 CIP-009-6 R2
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	FRCC's susceptibility to hurricanes and frequent storms, along with an extended growth season, increases the risk of vegetation related outages.	FAC-003-4 R6 & R7
Extreme Physical Events	The FRCC's peninsular geography along with its susceptibility to hurricanes, limited connections to the Eastern Interconnect and the existence of a significant SPS that could result in islanding increase the risk of an island event occurring.	PRC-006-3 R8 & R9 PRC-008-0 R1 & R2
Extreme Physical Events and Protection System Failures	The FRCC Region has SPS 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

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers risk elements (both ERO-wide and Regional) entity-specific risks, and other registered entity performance considerations, as well as

internal controls, to determine how an RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes Regional risk-based CMEP activities scheduled to occur during the 2018 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists all planned Audits for registered entities during the 2018 implementation year. The 2018 Compliance Audit Plan, located on the RE's website, details the registered entity's NERC Compliance Registry (NCR), registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

Throughout the implementation year, the RE will make updates to the 2018 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts Spot Checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on Regional risks and other considerations. The RE will follow the ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the ROP.

Self-Certification is a focused monitoring approach based on an entity's risk and may be conducted in lieu of a Spot Check or Audit. FRCC will perform Self-Certifications in 2018 over the implementation period (January 1 to December 31, 2017) on an annual basis for those NERC Reliability Standards that have been identified in the registered entity's COP. Registered entities will be notified during the fourth quarter of the NERC Reliability Standards and Requirements, the reporting worksheets, and the submittal methods for their respective Self-Certification(s). The registered entities are expected to complete the Self-Certification forms in the FRCC Compliance Tracking System, and upload all completed worksheets and associated evidence into the FRCC Secure Transfer Site.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the REs may also request data or information under Sections 800 or 1600 of the ROP; these data requests are not included on this schedule.

Compliance Outreach

Table A1.2: Compliance Outreach Activities

Outreach Activity	Anticipated Date
Spring Compliance Workshop (FRCC Combined O&P and CIP)	April 16-20, 2018
Fall Compliance Workshop (FRCC Combined O&P and CIP)	November 12-16, 2018
Reliability Standard Webinars	Periodic

Table A1.2: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
Additional Compliance Workshop (as needed)	TBD

Appendix A2: Midwest Reliability Organization (MRO) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- For 2018 compliance monitoring, MRO has been developing COPs for registered entities within its footprint. The goal of this effort is to provide multi-year COPs for each registered entity that contain monitoring scope, monitoring intervals, and monitoring methods.
- For all entities registered in MRO as of January 1, 2018, MRO's goal is to develop COPs by the end of 2018.

Other Regional Key Initiatives and Activities

- As part of the Annual IP, 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.
- 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 of 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 and Results

MRO's risk-based compliance monitoring efforts begin with assessments of risk at the ERO, Regional, and individual entity levels. In the annual ERO Enterprise CMEP IP, a set of continent-wide risks called ERO Risk Elements, and their associated NERC Reliability Standards and Requirements, are identified. While the Risk Elements are not a comprehensive list of all risks to the reliability of the BPS, they typically reflect the risks identified by the ERO as top-priority reliability risks as well as the Reliability Issues Steering Committee's (RISC) yearly ERO Priorities. Utilizing the ERO Risk Elements as a starting point, a comprehensive review of Region-specific risk called the Regional Risk Assessment (RRA) is then performed by MRO staff, with input and review by MRO technical committees, focusing on reliability risks specific to the MRO footprint. The RRA allows staff and entity SMEs to consider the ERO-identified risks at the regional level and serves as an opportunity to provide feedback to the ERO for risks that have been identified for the MRO regional footprint. This process includes factors and considerations such as footprint and registered entity characteristics, registered functions, geography, event analysis and misoperations, compliance history, and security considerations.

The highest-priority risks identified in the 2018 MRO RRA include decreasing numbers of IROLs, MRO's potential susceptibility to GMDs, new requirements for TOPs to perform Real-Time Analysis, market-based dispatch in planning studies, regional misoperation analysis, ride-through capability of inverter-based generation, and security vulnerabilities of entities lacking mature CIP programs, including staffing concerns.

Regional Risk Elements and Areas of Focus

The 2018 MRO RRA did not identify any additional regional Risk Elements or Areas of Focus to add to the suite of ERO Risk Elements. In order to ensure that the ERO Risk Elements as well as any significant risks recognized by the MRO RRA are addressed through a risk-based approach to compliance monitoring, MRO has developed Performance Areas. Performance Areas organize requirements according to the activities performed by entities in order to promote reliable operations of the BPS and simplifies the process of identifying those requirements that MRO plans to monitor in order to effectively address identified risks. The 2018 MRO Performance Areas list is available on MRO's website. Each Performance Area includes a description of the identified risk and a list of associated requirements that address those risks.

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers risk elements—both ERO-wide and Regional, entity-specific risks—and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2018 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists all planned Audits for registered entities during the 2018 implementation year. The 2018 Compliance Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2018 Compliance Audit Plan for this RE is located here: 2018 MRO Compliance Audit Plan on the MRO website. Throughout the implementation year, the RE may make updates to the 2018 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts Spot Checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the ROP.

For 2018, 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 NERC 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, to verify the accuracy of

the Self-Certification determinations. In the event further substantiation is needed, MRO staff may request additional evidence or include the applicable NERC Reliability 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 NERC Reliability Standards and Requirements.

As shown in Table A2.1, 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 NERC Reliability Standards that have been identified both through the RRA process and through 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, its compliance history, and other performance considerations.

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.

Table A2.1: 2018 Guided Self-Certification Schedule

Standard	Requirement	Quarter
NUC-001-3	R9	1
TOP-002-4	R3, R6, R7	2
CIP-008-5	R1, R2, R3	3
MOD-026-1	R2	3
MOD-027-1	R2	3
MOD-032-1	R1, R2, R3, R4	3
FAC-014-2	R2	4

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the RE may also request data or information under Sections 800 or 1600 of the ROP; these data requests are not included on this schedule.

Compliance Outreach

Table A2.2: 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 Reliability Conference	Twice a year (Spring and Fall)
MRO Security Conference	Fall 2018
MRO Compliance and Enforcement Program Conference	Fall 2018
Registered entity HEROs outreach events	At request of the entity
MRO Risk-Focused Conference or Training	Annually

Appendix A3: Northeast Power Coordinating Council (NPCC) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

- NPCC will continue to offer formal Operations and Planning (O&P) ICEs to all entities on the 2018 audit schedule.
- NPCC will also offer to perform CIP ICEs on entities that have already their initial CIP Version 5 audit.
- NPCC will refresh existing IRAs and use the 2018 ERO and NPCC IPs to scope 2018 monitoring engagements.

Other Regional Key Initiatives & Activities

- In 2018, NPCC will continue with a cyber security and physical security outreach program for volunteering entities.

Regional Risk Assessment Process and Results

NPCC considers the Risk Elements identified in the ERO Enterprise CMEP IP and the Risk Factors identified in the ERO Guide for Compliance Monitoring to identify important reliability risks within NPCC's footprint. If NPCC concludes that any of the ERO Risk Elements are not relevant reliability risks within NPCC's footprint, NPCC will provide documented rationale.

NPCC determines whether any additional regional risks specific to the NPCC footprint, but sufficiently different from the risks identified in the ERO Enterprise CMEP IP, should be added as Regional Risk Elements into the NPCC Implementation Plan. Input into Regional Risk Element determination can take the form of Enforcement trends, audit team observances, ERO or Regional events, issues raised by NERC or stakeholder groups, etc. Often, additional regional risks specific to the NPCC footprint may be categorized within a NERC-identified Risk Element and would not likely require an additional Regional Risk Element.

In the event NPCC identifies an additional Regional Risk Element that is not included in the ERO Enterprise CMEP IP, NPCC will provide justification and documentation regarding the additional Regional Risk Element.

In the development of the standards and requirements that appear in this Regional plan, NPCC considered the 2018 ERO Risk Factors and other tangible BES attributes such as entity functional registration, transmission assets, Remedial Action Schemes, Blackstart plans and facilities, generation assets, role of Underfrequency Load Shedding (UFLS) , Enforcement trends, historical events, etc.

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

NPCC did not identify any Regional Risk Elements for 2018.

Regional Risk Elements and Areas of Focus

Table A3.1 contains expanded ERO Risk Elements based on NPCC's Regional Risk Assessment process. The table also contains Areas of Focus to identified risks that may be considered in the development of a registered entity's COP.

Table A3.1: Additional Areas of Focus for ERO Risk Elements

Expanded ERO Risk Element	Justification	Associated Standard and Requirement(s)
Maintenance and Management of BPS Assets	NPCC will focus on coordination of relays and controls under several standards because inadequate/improper settings in these areas do not serve BES reliability. 1) Relay maintenance practices are imperative to continued BES reliability and there are frequent violations related to the PRC-005-6 implementation plan. 2) Although rarely used, UFLS schemes owned by the TO and DP are an extremely important aspect in limiting the extent of major disturbances. This is especially true in NPCC which has transmission corridors that are of the radial nature. As such, NPCC has a regional UFLS standard and will focus on the design and implementation of UFLS programs which are key in order to prevent a total system blackout like those that occurred in 1965, 1977, and 2003. In addition, the proper underfrequency settings at the GO directly correlate to the success of the UFLS program. 3) In 2017, NPCC documented an increase in not only non-compliance associated with generator voltage controls under PRC-019-2 and generator frequency/voltage relay settings under PRC-024-2, but also a steady flow of questions from entities. 4) NPCC will continue in the spirit of the 2010 Facility Rating Alert to audit and assess controls associated with FAC-008-3.	PRC-005-1.1b R1 (GO, TO, DP) PRC-005-6 R1 (GO, TO, DP) PRC-006-2 R3 (PC) R4 (PC) PRC-006-NPCC-1 R4 (TO, DP) R7 (TO, DP) R13 (GO) PRC-019-2 R1 (GO, TO) FAC-008-3 R3 (GO, TO)
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 include 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.	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

Table A3.1: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	RC backup control centers with the functionality of the primary control center further ensure interconnection reliability and a more secure recovery from the loss of the primary.	R3 (RC)
Extreme Physical Events	The ability to mitigate the effects of 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 R2 (RC)
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 experiencing/foreseeing a transmission problem; performing next day analyses; performing 30-minute assessments; implementing real-time time actions to both prevent in advance and mitigate in real-time all 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-002-4 R1 (RC) R2 (RC) IRO-008-2 R1 (RC) R2 (RC) R5 (RC) IRO-009-2 R2 (RC) TOP-001-3 (until 6/30/18) TOP-001-4 (effective 7/1/18) R7 (TOP) R15 (TOP) R16 (TOP) R18 (TOP) R19 (TOP) TOP-002-4 R1 (TOP) R6 (TOP)

Table A3.1: 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 gain 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, R6, R7 (RC, BA, TOP) R3, R6 (GOP, DP) PER-005-2 R1 (RC, BA, TOP) R2 (TO) R3 (TO)

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers Risk Elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2018 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists all planned Audits for registered entities during the 2018 implementation year. The 2018 Compliance Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2018 Compliance Audit Plan for NPCC is located here: NPCC Compliance Audit Plan. Throughout the implementation year, the RE will may make updates to the 2018 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts Spot Checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a 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 performing an Audit.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the ROP.

As shown in Table A3.2, NPCC will perform guided Self-Certifications on a quarterly basis in 2018, with a 45-day advance notice given to the entity. The entity will receive the notice of the requirement covered by the guided Self-Certification and will be instructed to submit their compliance documentation into the NPCC compliance portal. There are specific requirements that will undergo a guided Self-Certification for each quarter. Only a subset of the entities registered for the function that applies to the chosen requirement will receive the guided Self-Certification notification in the particular quarter.

Table A3.2: Guided Self-Certification Schedule

Quarter 1				
Standard	**Requirement**	**Function**	**Notification Date**	**Due Date**
PER-005-2	R6	GOP	January 9	February 23
PRC-024-2	R2	GO	January 9	February 23
Quarter 2				
Standard	**Requirement**	**Function**	**Notification Date**	**Due Date**
PRC-006-NPCC-1	R4, R7	DPUF	March 27	May 11
PRC-005-6	R1, R2, R3	DPUF	March 27	May 11
Quarter 3				
Standard	**Requirement**	**Function**	**Notification Date**	**Due Date**
VAR-002-4	R1	GOP	June 26	August 10
PRC-019-2	R1	GO	June 26	August 10
Quarter 4				
Standard	**Requirement**	**Function**	**Notification Date**	**Due Date**
PRC-006-NPCC-1	R4, R7	DPUF	September 25	November 9
PRC-005-6	R1, R2, R3	DPUF	September 25	November 9

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the REs may also request data or information under Sections 800 or 1600 of the NERC ROP; these data requests are not included on this schedule.

Compliance Outreach

Table A3.3: 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 2018 November 2018
Introduction to NPCC for Beginners – NPCC provides an introductory class for those new to CMEP activities prior to the May and November workshops.	May 2018 November 2018
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 2018 November 2018
CIP and O&P 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 2018 November 2018
Cyber Security Outreach for Non-Nuclear Generators – This will provide guidance to non-nuclear sites on all facets of their on-site cyber security.	Throughout 2018
Physical Security Outreach for Non-Nuclear Generators – This will provide guidance to non-nuclear sites on all facets of their on-site physical security.	Throughout 2018
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 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.	

Table A3.3: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
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) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

ReliabilityFirst will support the ERO Program Alignment initiative, and follow and perform the ERO Risk-Based Compliance Oversight Framework described in the ERO Enterprise CMEP IP. The 2018 ERO Enterprise CMEP IP identifies a number of Risk Elements and Areas of Focus, which provide a starting point for ReliabilityFirst's risk analysis and COP development. However, the 2018 ERO Enterprise CMEP IP recognizes that it does not include the complete set of risks that may affect the BPS that Regional Entities are expected to consider (local risks and specific circumstances associated with individual registered entities within their footprint) when developing their COPs.

To account for such risks and circumstances, ReliabilityFirst performed its Regional Risk Assessment, which identified risks within the ReliabilityFirst region. ReliabilityFirst may monitor the NERC Reliability Standards and Requirements associated with these risks, which are referred to as the 2018 ReliabilityFirst Risk Elements, in 2018. ReliabilityFirst also has the discretion to add, subtract, or modify NERC Reliability Standards and Requirements in its COPs for individual registered entities as it deems necessary based on the individual registered entity IRA and COP development.

ReliabilityFirst monitors 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 2018. A guided Self-Certification requires an entity to submit their supporting documentation to substantiate their self-assessment. 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 in the year. Guided Self-Certifications focus on specific risks and 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. To that end, ReliabilityFirst will continue to exercise professional judgment in enforcement by processing qualified minimal-risk noncompliance as compliance exceptions. Since the implementation of risk-based enforcement, most minimal-risk noncompliances have been processed as compliance exceptions, and ReliabilityFirst expects that trend to continue.

There are two ways in which a minimal risk noncompliance may qualify for compliance exception treatment: 1) on a case-by-case basis based on the facts and circumstances of a particular noncompliance; and 2) via a presumption of compliance exception treatment based on self-logging privileges that ReliabilityFirst grants to a registered entity. Self-logging privileges are awarded to registered entities based on the registered entity's demonstrated ability to identify, assess, and correct noncompliances in addition to other factors.

ReliabilityFirst will also continue to use the Find, Fix, Track ("FFT") disposition method for moderate-risk issues or minimal-risk issues that ReliabilityFirst determines are otherwise inappropriate for compliance exception treatment.

Compliance exceptions and FFTs are both streamlined enforcement dispositions. The main difference between compliance exceptions and FFTs is that compliance exceptions do not become part of an entity's formal violation history and thus will not be a basis for aggravating a penalty for a future violation.

Penalties will generally be reserved for situations involving multiple serious-risk violations or programmatic failures. Additionally, penalties may be appropriate as a result of even a small number of serious- or moderate-risk violations depending on the circumstances—including, for example, the method of identification of the violation, the duration of the violation, and an entity's compliance history.

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. 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.

Regional Risk Assessment Process and Results

The Regional Risk Assessment identifies risks within the ReliabilityFirst Region that could potentially impact the reliability of the BPS. To accomplish the Regional Risk Assessment, ReliabilityFirst utilizes a cross-functional team of internal SMEs (the Regional Risk Assessment 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 Regional Risk Assessment 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, SOLs, IROLs, 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 Regional Risk Assessment team develops the results of the Regional Risk Assessment in the form of ReliabilityFirst Risk Elements.

ReliabilityFirst may include additional detail on the ReliabilityFirst Risk Elements and their associated NERC Reliability Standards and Requirements in the 2018 registered-entity-specific COPs.

The Regional Risk Assessment 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 Regional Risk Assessment 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 CIP and 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 affect its risk to the BPS.

In addition to the Risk Elements and Focus Areas identified from the Regional Risk Assessment and the ERO Enterprise common Risk Factors, ReliabilityFirst considers the following information when developing IRAs and COPs:

- *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* - Set forth in Appendix C to the "2014 ERO Inherent Risk Assessment Guide"
- *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* - Set forth in Appendix B to the "2016 ERO Enterprise Guide for Risk based Compliance Monitoring"

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 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 NERC 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 2017 ReliabilityFirst RRA has identified the following ReliabilityFirst Risk Elements, applicable for 2018, which align with NERC's 2018 ERO Risk Elements and therefore constitute Expanded ERO Risk Elements. They are:

- 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
- Cyber Security - Supply Chain Risk Management

With this, CIP – "Cyber Security - Supply Chain Risk Management" is identified as a "ReliabilityFirst" Risk Element to ensure Regional focus while the development of the associated CIP-013 standard is completed, approved, and implemented in industry.

Table A4.1 contains the Regional Risk Elements that ReliabilityFirst identified during the Regional Risk Assessment process. Also, as a result of ReliabilityFirst's review of the NERC Risk Elements and the ReliabilityFirst Risk Elements, ReliabilityFirst identified the associated NERC Reliability Standards and Requirements, listed in Table A4.1, for increased compliance monitoring focus in 2018. Thus, ReliabilityFirst justified the inclusion of these NERC Reliability Standards and Requirements during the Regional Risk Assessment. In Table A4.2, ReliabilityFirst provides *additional justifications where applicable.* These NERC Reliability 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: NERC Reliability Standards and Requirements in BLUE denote their inclusion in both this Appendix and the main document (the 2018 ERO Enterprise CMEP IP).

Table A4.1: Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Critical Infrastructure Protection: - Cyber Security Supply Chain Risk Management	Cyber Security Supply Chain Risk Management of industrial control system hardware, software, and computing and networking services associated with BES operations is crucial. Therefore, monitoring the implementation of security controls for Cyber Security Supply Chain Risk Management of BES Cyber Systems is a focus going forward to ensure effective controls and mitigation are in place. Although CIP-013-1 is still under development, ReliabilityFirst is including this ReliabilityFirst Risk Element for 2018. The purpose of providing it in the IP is to keep this risk in front of our registered, so entities are taking mitigating steps to address the risk even though the Standard is not yet in place.	CIP-013-1, Requirements To Be Defined

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and 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 2016-2017 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. For example, icing/clogging of combustion turbine inlet filters still continues to be a common problem for some combined-cycle plants.	EOP-011-1 R1,R2 TOP-002-4 R2,R4,R5 TOP-003-3 R1,R2,R5 TPL-001-4 R2
Extreme Physical Events: - Extreme Natural Events Maintenance and Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) to monitor operating conditions in ReliabilityFirst's footprint during unusually hot weather conditions and extreme cold weather conditions. The ISO/RTOs took steps to prepare for winter operations. These steps included drills to examine incidents that could impact reliability; studying "worst-case" scenarios such as impacts to gas pipeline failures; ensuring communication	EOP-005-2 R1,R1.2 EOP-011-1 R1,R2 FAC-011-3 R3,R4 (Part 4.3) FAC-014-2 R1,R2 IRO-001-4 R1,R2,R3 IRO-002-4 R3,R4 IRO-008-2 R1,R3,R4,R5,R6

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Monitoring and Situational Awareness Event Response/Recovery Planning and System Analysis	and coordination with natural gas line suppliers; working with generator owners on cold weather preparedness, fuel inventory survey, resource testing and emergency procedure drills; and higher expectations for generator capacity performance. No significant winter-related events were encountered that impacted the reliability of the BES. Regarding summer weather conditions, some areas of the ReliabilityFirst footprint experienced severe storms with high winds, rain, and lightning, which resulted in customer outages ranging from 30,000 to 70,000. No significant hot weather-related events were encountered that impacted the reliability of the BES. The ISO/RTO capacity levels continue to exceed the forecasted peak demand and reserve margin requirement. Recent history has revealed flatter load growth driven by a number of factors. MISO's demand forecasts show an overall negative load growth. PJM's most recent 2017 load forecast report projects summer peak load growth for the RTO to average 0.2 percent per year over the next 10 years. PJM research indicates that several evolving customer behaviors are driving flatter load growth: more efficient manufacturing equipment and home appliances, and distributed energy resources such as behind-the-meter rooftop solar installations.	IRO-009-2 R2,R3 NUC-001-3 R4 PER-005-2 R1,R2 TOP-001-3 R3,R4,R8,R10,R11,R12, R13,R14 TOP-002-4 R1,R2,R4,R5 VAR-001-4.1 R2
Event Response/Recovery Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) because TOPs' 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 TOPs in the ReliabilityFirst footprint. EOP-005-2, R6 focuses on verifying that the TOP'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 TOPs 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 GMD events. GMD events can result in the loss of power transformers,	EOP-010-1 R1,R2,R3 TPL-007-1 R1,R2,R3,R4,R5,R6,R7 - Effective dates

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	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. Planners should be working with their entities to gather system data, perform the network analyses, and develop corrective action plans, as necessary for GMD events. Both the planners and assets owners should perform the necessary calculations as input to thermal heating assessments of applicable transformers. Grid Resilience Going forward, resilience should be embedded to an even greater extent in transmission expansion plans to further enhance existing facility performance. Planning metrics should be expanded to grid resilience and consider an evaluation of wide area events affecting the transmission system and back-to-back system element loss due to events such as the loss of a tower line with three or more circuits, loss of transmission lines on a common right of way, misoperation of a special protection system, etc.	staggered over five-year period.
Planning and System Analysis	ReliabilityFirst is expanding the ERO risk element(s) because, with the role of the PA, PC, and TP 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 PA and PC and TPs. ReliabilityFirst has determined that because of the nature of its footprint, with two large PAs and PCs working in conjunction with the TPs, 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. Grid Resilience Going forward, resilience should be embedded to an even greater extent in transmission expansion plans to further enhance existing facility performance. Planning metrics	TPL-001-4 R1,R2,R3,R4,R5,R6,R7, R8

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	should be expanded to grid resilience and consider an evaluation of wide area events affecting the transmission system and back-to-back system element loss due to events such as the loss of a tower line with three or more circuits, loss of transmission lines on a common right of way, misoperation of a special protection system, etc.	
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. If formally submitted deactivation plans materialize, more than 25,000 MW of coal-fired generation will have deactivated between 2011 and 2020. Generator deactivations alter power flows that can cause transmission line overloads and, given reductions in system reactive support from those generators, can undermine voltage support. While some renewable resources can operate continually like conventional fossil-fueled power plants, others powered by wind and solar operate intermittently. Wind turbines can generate electricity only when wind speed is within a range consistent with turbine physical specifications. This presents challenges with respect to real-time operational dispatch.	BAL-003-1.1 R1,R2,R3,R4 BAL-005-0.2b R17 EOP-004-3 R2 EOP-011 -1 R1,R2,R6 IRO-001-4 R1,R2,R3 IRO-002-4 R3,R4 IRO-008-2 R2,R6 IRO-010-2 R1 (Part 1.2), R3 IRO-017-1 R1 PRC-006-2 R1,R2,R3,R4,R5, R9,R10 PRC-010-2 R1,R4,R5 TOP-001-3 R8,R10,R11,R12,R13,R14,R15,R18 TOP-002-4 R1 TOP-003-3 R1 TPL-001-4 R1,R2,R3,R7 VAR-002-4 R2,R3,R4
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	CIP-006-6 R1,R2,R3 CIP-014-2 R1,R2,R3,R4,R5,R6

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	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.	
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 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, and providing appropriate level of awareness towards protecting and accessing BES Cyber Systems are included.	CIP-003-6 R1, Part 1.1 CIP-004-6 R1,R2,R3,R4,R5 CIP-005-5 R1,R2 CIP-006-6 R1,R2 CIP-007-6 R1,R2,R3,R4,R5 CIP-011-2 R1,R2
Maintenance and Management of BPS Assets Human 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 standards in the ReliabilityFirst footprint. Need to focus on Generator Owners since ~50 percent of relay operations result in a misoperation.	PRC-005-6 R1,R2,R3,R4,R5
Human Performance	ReliabilityFirst is expanding the ERO risk element(s) because GOPs continue to experience deviations in voltage schedules and sometimes fail to notify the TOPs since VAR-002 remains one of the most violated standards in the ReliabilityFirst footprint. The root causes of these deviations and notice failures vary.	PER-005-2 R6 VAR-002-4 R1,R2,R3

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Human Performance - Training - Lack of awareness to CIP - Process deficiency	ReliabilityFirst is expanding the ERO risk element(s) because Entities in ReliabilityFirst region continues to experience issues with root causes centered on human performance error, lack of understanding/awareness to CIP standards and requirements. Many violations/failures involving these root causes warrant increased focus.	CIP-003-6 R1, R2 Attachment 1 Sec.1 CIP-004-6 R1,R2
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 be changes of restoration resources, which require restoration plan updates.	COM-002-4 R1,R2,R3,R4 EOP-005-2 R10,R11,R17 EOP-006-2 R9,R10 EOP-011-1 R1,R2
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 warrant increased focus. Need to focus on GOs since ~50 percent of relay operations result in a misoperation.	FAC-010-2.1 R2.2 PRC-001-1.1(ii) R2, R2.1,R2.2 PRC-004-5(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.	IRO-002-5 R3 IRO-010-2 R3 TOP-001-3 R10,R11 TOP-003-3 R5
Maintenance and Management of BPS Assets	ReliabilityFirst is expanding the ERO risk element(s) because the ReliabilityFirst entities continue to address aging infrastructure. Some TOs have added aging transmission line replacement to their planning criteria. Over the past several years, it has been observed that TO criteria and aging infrastructure in particular are increasingly driving the need for baseline projects. Many 500 kV lines were constructed in the 1960s; 230 kV and 115 kV lines date to the 1950s and earlier. Over the past several years, TOs have begun to address aging infrastructure concerns, specifically for transformers and transmission lines. The ReliabilityFirst entities should annually refresh their probabilistic risk assessments of EHV transformers to confirm replacement strategies and timing.	FAC-003-4 R1,R2,R6,R7 PRC-005-6 R3,R4 PRC-008-0 R1,R2 PRC-011-0 R1 PRC-017-0 R1

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
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. Recent years have witnessed a significant ramp-up in behind-the-meter distributed solar resources: rising over 2,500 MW since 1998, with more than 95 percent of installations since 2010. Though not a large amount from an RTO perspective, certain areas of the ReliabilityFirst footprint contain significant concentrations. An unprecedented capacity shift driven by federal and state public policy and broader fuel economics continues to be managed due to: • New generating plants powered by Marcellus and Utica shale natural gas. • New wind and solar units driven by federal and state renewable incentives. • Generating plant deactivations. • Market impacts introduced by demand resources and energy efficiency programs. MISO - Wind energy is the most prevalent renewable energy resource in the MISO footprint. Wind capacity in the MISO footprint has increased exponentially since the start of the energy market in 2005. Beginning with nearly 1,000 MW of installed wind, the MISO footprint now contains 15,106 MW of total registered wind capacity as of May 2016. Approximately 8 GW of currently unannounced coal retirements are expected in the next 15 years. That value could potentially triple depending on carbon regulations. PJM - As for coal, if formally submitted deactivation plans materialize, more than 25,000 MW of coal-fired generation will have deactivated between 2011 and 2020.	BAL-002-1 R1 EOP-011-1 R2,R6 IRO-002-5 R3 TPL-001-4 R1,R2 VAR-001-4.1 R2
Critical Infrastructure Protection: - System Downtime	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	EOP-005-2 R10,R11,R17 EOP-006-2 R9,R10

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
Event Response/Recovery (With a focus on RESILIENCY)	continue 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 Blackstart restoration efforts, drills, training, ReliabilityFirst identified EOP-005, EOP-006, CIP-008-5 and 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.	CIP-008-5 R1,R2,R3 CIP-009-6 R1,R2,R3 CIP-014 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-004-3 R2 EOP-008-1 R1 IRO-002-5 R3 IRO-010-2 R3 TOP-001-3 R10,R11,R12,R13,R14 TOP-003-3 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	MOD-025-2 R1,R2,R3 PRC-019-2 R1,R2

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	essential for the modeling, analysis, and reliable operation of the BPS.	
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. ReliabilityFirst has identified inconsistences with Facility Ratings in operations and during monitoring engagements of registered entities. FAC-008 remains in the top 10 violated standards in the ReliabilityFirst footprint.	FAC-008-3 R1,R2,R3
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,R2,R3 CIP-010-2 R1,R2,R3,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	CIP-002-5.1 R1,R2

Table A4.2: Additional Areas of Focus for ERO Risk Elements		
Expanded ERO Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	compromises that could lead to misoperation or instability in the BES.	
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 ReliabilityFirst 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 CIP-003-6 R2 - Attachment 1 Sec.1-4 CIP-003-6 R3, R4

Regional Compliance Monitoring Plan

Compliance Audits

ReliabilityFirst intends to conduct 14 on-site CIP Audits in 2018, and may conduct additional Audits as necessary. Most of the 14 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 14 Audits are MRRE Audits under the Coordinated Oversight Program, and ReliabilityFirst is the LRE for two 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 2018 to arrange schedules and confirm the Audit engagements.

With the effective date for the substantive low impact requirements for identifying and securing sites that possess Low Impact External Routable Connectivity not being until September 1, 2018, ReliabilityFirst anticipates assessing with the possibility of performing reviews on low impact only entities in 2019. At that time, ReliabilityFirst will use an internal risk-based assessment to select a subset of all those owners of only low cyber systems and conduct monitoring of those entities.

ReliabilityFirst intends to conduct 60 O&P engagements in 2018, but may conduct additional engagements as necessary. These engagements are being conducted pursuant to the ROP and include registered entities that must be audited every three years. Of the 60 Audits, 6 are MRRE engagements in which 2 will be led by another Regional Entity. ReliabilityFirst has already contacted the registered entities being audited in 2018 to arrange schedules and confirm the audit engagements.

The 2018 Compliance Audit Plan for this RE is posted on the ReliabilityFirst Website.

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 that 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.

Spot Checks

ReliabilityFirst may schedule Spot Checks in 2018, 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. The RE will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a Spot Check.

Self-Certifications

ReliabilityFirst will perform guided Self-Certifications as needed throughout in 2018. 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.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the REs may also request data or information under Sections 800 or 1600 of the ROP; these data requests are not included on this schedule.

ReliabilityFirst used this schedule to develop a Compliance Monitoring Schedule that contains the NERC Reliability Standards and Requirements for the Periodic Data Submittals scheduled for 2018. 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.

Compliance Outreach

Table A4.3: 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

Table A4.3: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
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 (Columbus: April 24- 26, 2018 and Independence: September 25-27, 2018)
CIP Outreach and Awareness – ReliabilityFirst will conduct CIP outreach, including training and education engagements, to ensure that registered entities have confidence in their implementation of the CIP Standards and Requirements. These engagements will primarily be conducted as Workshops and Webinars.	Sessions are held as requested by our registered entities, built into the workshop material and or addressed though our Assist Visit program
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
Periodic Reports - ReliabilityFirst will provide Periodic Reports to its registered entities identifying compliance-related activities with which the registered entities continue to struggle. These reports will be posted on the ReliabilityFirst website.	Monthly throughout the year
Monthly Reliability and Compliance Forum Calls - ReliabilityFirst has instituted a monthly conference call to provide an open forum for registered entities to call and voice concerns, ask questions, and gain information about upcoming compliance items. The calls are also used to share reliability issues, trends, and information related to existing or emerging risks. These calls were previously called our Open Compliance Calls, but in 2018 we are repurposing these calls to focus on reliability and compliance issues.	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

Table A4.3: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
CIP Low Impact Focus Group - The CIP Low Impact Focus Group consists of entities in the ReliabilityFirst footprint who are responsible for compliance for low impact BES Cyber Systems. The group holds monthly meetings to discuss various topics, and holds periodic webinars with featured speakers. The goals of the group include the following: • Assist registered entities with CIP low-impact assets • Communicate lessons learned from high- and medium-impact entities • Communicate lessons learned from other Regions • Provide a forum for general questions • Provide a forum to communicate good practices	Monthly throughout the year
MKInsight Entity Profile - ReliabilityFirst will request its registered entities to report entity-specific information, using an internet-based compliance monitoring application.	Updated yearly or throughout the year as needed

Appendix A5: SERC Reliability Corporation (SERC) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

NERC CMEP tools used by SERC in 2018 will include Compliance Audit, Spot Check, and Guided Self-Certification. SERC will focus its resources on higher-risk items primarily identified through entity-specific IRAs. SERC will continue to consider an outreach component to on-site Compliance Audits, as well as assessing any internal controls. During the on-site week, the entity may engage SERC compliance audit staff to address approaches and ask questions in both the O&P and CIP compliance areas. SERC continues to enhance its Frequently Asked Questions process, where SERC SMEs address questions asked by entities.

SERC continues to look for ways to strengthen reliability, reduce risk to the BES, and promote a culture of reliability excellence. Past compliance monitoring activities identified discrepancies between Facility Ratings and the ratings used in system operations. SERC will continue to review operational ratings and compare those ratings to the Facility Ratings developed in accordance with Registered Entity Facility Rating methodologies. In addition, SERC plans to conduct asset reviews in the field by inspecting substations and generating facilities, to verify that Equipment Ratings used to develop Facility Ratings match the actual equipment in the field. SERC auditors will verify these ratings during control center tours by comparing EMS values to stated Facility Ratings. Failure of registered entities to properly develop and apply Facility Ratings can produce incorrect SOLs and lead to damage of BES equipment.

Reviews of internal controls during compliance monitoring activities will continue to mature throughout 2018. SERC completed the IRAs for entities registered as RCs, BAs, and TOs in 2016. SERC will complete an IRA on all entities registered before October 1, 2017 by the end of 2017. SERC will continue to develop a registered entity's COP based on the risks identified during the IRA process, entity performance data, and Regional trends.

Other Regional Key Initiatives & Activities

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.

SERC will continue to promote and support the MRRE program in 2018. As an LRE, SERC will lead efforts related to all aspects of the CMEP. The LRE coordinates and conducts the IRA, with input from each ARE, and determines the appropriate COP. This coordinated oversight should eliminate unnecessary duplication of compliance monitoring and enforcement activities. In addition, as the ARE, SERC will continue to collaborate and coordinate with the LREs to ensure IRAs, compliance monitoring, and enforcement activities include SERC Regional considerations.

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, 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 and Results

Reliable operation of the 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 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 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 NERC 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

Table A5.1 contains the regional risk elements, and expanded ERO risk elements, for focus during 2018 based on the Regional Risk Assessment process. The table also contains areas of focus to identified risks that may be considered in the development of a registered entity's COP.

Table A5.1: Regional Risk Elements

Regional Risk Element	Justification	Associated Standard and Requirement(s)
Severe weather events and impacts on transmission and generation	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 assessment of SERC Performance Information for Identifying Potential Reliability Risk, as well as through the NERC Reliability Assessment reporting process. SERC is expanding the NERC area of focus based on operational risks, such as deficient entity response and performance, identified during severe 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-002-2 R1 BAL-005-0.2b R7 COM-002-4 R1, R2, 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 R2, R3, R4 IRO-003-2 R1, R2 IRO-004-2 R1

Table A5.1: Regional Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	• Insufficient coordinated studies • Insufficient coordinated operations • Uncertainty of resources and resource mix • Available generator ability to adequately respond to frequency changes SERC's unique PC structure necessitates coordination throughout the SERC Region. There are a large number of PCs 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.	PRC-001-1-1.1(ii) R3, R4, R5 PRC-019-2, R1, VAR-002-4 R1, 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

Table A5.2: Additional Areas of Focus for ERO Risk Elements		
Expanded Risk Elements	**Justification**	**Associated Standard and Requirement(s)**
Critical Infrastructure Protection	The area of critical infrastructure protection remains an area of significant importance. SERC is expanding this NERC area of focus due to the risk of cyber security controls for BES cyber systems being compromised, and leading to unauthorized electronic access to those systems; extreme physical events including sabotage,	CIP-003, R2 CIP-007, R4 CIP-010-2, R1, R3, R4

Table A5.2: Additional Areas of Focus for ERO Risk Elements		
Expanded Risk Elements	**Justification**	**Associated Standard and Requirement(s)**
	attacks, and vandalism; and introduction of widespread malware.	
Maintenance and Management of BPS Assets	SERC is expanding this NERC area of focus based on operational risks, and trends in misoperations in SERC. Also SERC's 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-003-4, R3 PRC-004-5, R2, R3, R4

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks and other registered entity performance considerations, as well as internal controls, to determine how an RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes Regional risk-based CMEP activities occurring during the 2018 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists all planned Audits for registered entities during the 2018 implementation year. The 2018 Compliance Audit Plan, located on the RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2018 Compliance Audit Plan for this RE is located on SERC's website. Throughout the implementation year, the RE will may make updates to the 2018 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts Spot Checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events; to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals; or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the ROP for notifying registered entities of any Self-Certifications, ensuring advance notice according to the ROP.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the REs may also request data or information under Sections 800 or 1600 of the ROP; these data requests are not included on this schedule.

Compliance Outreach

Table A.2: 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 Events Calendar on the home page or under Outreach > Events Calendar. Outreach events are promoted in the monthly SERC Transmission newsletter and email notifications; reminders are sent to primary and alternate compliance contacts for all registered entities within the SERC Region footprint.	
• Open Forum (WebEx)	Jan 29, 2018
• Spring Compliance Seminar (Charlotte, NC and WebEx)	Mar 6-7, 2018
• Small Entity Seminar (Charlotte, NC and WebEx)	Mar 7, 2018
• Open Forum (WebEx)	May 21, 2018
• Open Forum (WebEx)	Jul 30, 2018
• CIP Compliance Seminar (Charlotte, NC and WebEx)	Sep 19-20, 2018
• Fall Compliance Seminar (Charlotte, NC and WebEx)	Oct 10-11, 2018
Focused Workshops and Webinars Supplemental focused events scheduled on an as-needed basis provide outreach and training for new or revised NERC Reliability Standards, targeted groups of registered entities based on functional registration, and ERO initiatives.	As needed throughout the year
FAQ & Lessons Learned SERC staff SMEs 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.	Available throughout the year
Compliance Outreach Assistance A new SERC 101 webpage will be online by November 1, 2017. Upon completion, a *Welcome to SERC* email will be sent to newly registered entities. The new webpage will also be promoted in each issue of the *SERC Transmission* newsletter. The webpage will contain links to basic compliance information on the FERC, NERC, and SERC websites in one convenient location. A sample of the links includes information such as the Energy Policy Act (EPA) of 2005 and the FERC Reliability Primer 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.	Nov 1, 2017 Available throughout the year thereafter

Table A.2: Compliance Outreach Activities	
Outreach Activity	**Anticipated Date**
SERC Transmission Newsletter The SERC Transmission newsletter is distributed monthly to registered entities within the SERC Region, ERO Enterprise stakeholders, and all interested persons who request a subscription. It is also posted on the SERC website. Articles contain links to scheduled outreach information for both SERC and NERC events and includes news items from FERC, NERC, and SERC. It also includes other topics helpful to maintaining BPS reliability.	Distributed monthly and available throughout the year on the SERC website
SERC Compliance Portal SERC registered entities submit Self-Certifications, Self-Reports, Mitigation Plans, and Data Submittals via the SERC Portal. Feedback from targeted surveys allows SERC to incorporate enhancements based on the needs of the users, and outreach events include training on upgrades and enhancements.	Available 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. Responses to emails are to be sent within 24 hours. When a response will take longer than 24 hours, an acknowledgement email is sent to ensure the sender that SERC has received the inquiry and someone will respond as soon as possible.	Monitored throughout the year

Appendix A6: Southwest Power Pool Regional Entity (SPP RE) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

On March 5, 2018, NERC filed a joint petition with the FERC regarding the dissolution of SPP RE, requesting to terminate the Regional Delegation Agreement between NERC and SPP. [30] In the FERC petition, NERC, SERC, MRO, and SPP RE proposed transfers of registered entities in the SPP RE footprint to MRO and SERC by July 1, 2018. SPP RE is coordinating with SERC, MRO, and NERC to ensure it carries out planned CMEP activities through July 1, 2018.

Subject to regulatory approval, registered entities transferring to the MRO and SERC REs should follow the revised Regional IPs for SERC and MRO. Additionally, as detailed in below sections, SPP RE will not conduct Periodic Data Submittals and Self-Certifications beyond Q1 2018.

During 2018, SPP RE will:

- Perform the responsibilities and duties as described in the annual ERO Enterprise CMEP IP.
- Continue to engage the registered entities that request an ICE or Self-Logging.
- Continue to implement the Coordinated Oversight Program for the MRREs.
- Continue to develop and refine the tools and templates used for compliance monitoring, IRAs, and ICEs.
- Perform internal reviews of compliance monitoring for the purpose of improving the SPP RE compliance and enforcement oversight program.

SPP RE will perform a review and update of the IRAs for the registered entities that are identified in the 2018 Monitoring schedule.

Other Regional Key Initiatives & Activities

SPP RE will 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 and Results

The SPP RE's 2018 Regional Risk Assessment is to identify risks at the regional level that will impact the compliance monitoring activities in 2018. SPP RE staff evaluated regional data, trends, geography, events, violations, and other regionally identified risk. Based on the assessment, SPP RE determined the following regional risks:

- Misoperations due to a high percentage of misoperations-to-operations within the SPP RE footprint; automatic voltage controls based on the violations due to change of maintaining voltage schedules;
- Automatic Voltage Regulator (AVR) status and TOP notification;
- Patch Management due to failing-to-track, evaluating and installing cyber security patches for applicable Cyber Assets; and

[30] March 5, 2018 FERC Filing for SPP RE Dissolution.

- Not generating alerts for all events for identification of, and after-the-fact investigations of, Cyber Security Incidents. Specifically, if the logging method stopped but the machine was still online, no alerts would be issued.

These Regional Risks are included in the 2018 ERO Risk Elements.

Regional Risk Elements and Areas of Focus

SPP RE did not identify any Regional Risk Elements for 2018, nor did SPP RE determine a need to expand on the 2018 ERO Enterprise Risk Elements and Areas of Focus.

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks, and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes Regional risk-based CMEP activities occurring during the 2018 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists all planned Audits for registered entities through July 1, 2018. The 2018 Compliance Audit Plan, located on the SPP RE's website, details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The current 2018 Compliance Audit Plan for SPP RE is located here: Spp.org>Regional Entity Home>Compliance and Enforcement>2018 Compliance Documents. SPP RE will follow the NERC ROP to update the 2018 Compliance Audit Plan, which includes approval by NERC and notification to registered entities of changes.

Spot Checks

SPP RE has no planned spot checks through July 1, 2018.

Self-Certifications

The SPP RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The SPP RE will follow the ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the ROP.

In addition, SPP RE will continue to require certain 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 NERC 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. SPP RE conducts Self-Certifications using webCDMS.

SPP RE will conduct Q1 2018 Self-Certifications for the submission period of January 1, 2018 to April 2, 2018. SPP RE will not conduct Self-Certification activities after Q1 2018.

The SPP RE follows the Q1, 2018 self-certification schedule posted at Spp.org>Regional Entity Home>Compliance and Enforcement>2018 Compliance Documents.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. SPP RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the REs may

also request data or information under Sections 800 or 1600 of the ROP; these data requests are not included on this schedule. Registered entities within the SPP RE footprint should continue to follow the instructions within SPP RE's 2018 Compliance Reporting Schedule for Q1 2018.

Compliance Outreach

Table A6.1: Compliance Outreach Activities

Outreach Activity	Anticipated Date
SPP RE Newsletters	Monthly
SPP.org RE Webpage	Updated as needed
2018 Spring Compliance Workshop	March 27, 2018
2018 CIP Workshop	June 5, 2018
Webinars and Training Videos	As developed
Event Analysis Lessons Learned	As developed

Appendix A7: Texas Reliability Entity (Texas RE) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

In 2017, Texas RE continued to evaluate the risk-based compliance monitoring implementation efforts and continued to facilitate improvements in effectiveness and efficiency. Every registered entity selected for an engagement in 2018 will undergo an IRA to focus efforts on reliability risks for the registered entity and provide focus for Texas RE staff.

Texas RE will follow the ROP requirements for notifying candidates once a CMEP Tool, as developed within the approved ERO Enterprise Risk-Based Compliance Oversight Framework, is determined. The ROP require that an RC, BA, or a TOP will have an Audit performed "at least once every three years". Those RCs, BAs, or TOPs meeting the "at least once every three years" designation will be listed in the Compliance Audit Plan.

During the year, Texas RE may update the IP. 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 matters deemed appropriate by Texas RE or NERC. When updates occur, Texas RE will submit updates to NERC, which will review and act on any proposed changes. NERC is responsible for updating the ERO Enterprise 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 O&P Requirements and CIP Requirements concurrently during engagements rather than approaching Requirements relative to the risks separately.

As part of risk-based CMEP implementation, Texas RE further enhanced its in-house IRA tool. The IRA tool will continue to undergo improvements based on the ERO Enterprise Guide for Compliance Monitoring, NERC oversight feedback, lessons learned, registered entity feedback, and the straightforward common sense approach of the Texas RE Risk group. During 2018, every registered entity engagement will start with an IRA, the results of which will be used to develop appropriate oversight and will be provided to the registered entity as an IRA Summary Report.

Other Regional Key Initiatives & Activities

Texas RE will support NERC management in preparations for the implementation of the Supply Chain Standards (CIP-005-6, CIP-010-3, and CIP-013-1).[31] Texas RE will continue its collaborative effort among NERC, the Regional Entities, and registered entities to identify and implement changes that enhance the effectiveness of the CMEP.

Regional Risk Assessment Process and Results

The Regional Risk Assessment process is a facet of Texas RE's efforts to adequately plan effective compliance monitoring in the ERCOT 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 BES risks), completing an ICE (entity-level risk mitigation), and developing a 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.

[31] NERC Board of Trustees Resolution - Supply Chain Standard as reviewed during the August 10, 2017 Board of Trustees meeting

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 created reports, both locally and nationally, and discussions focusing on reliability risks. The ERO Enterprise Guide for Compliance Monitoring (Guide) provides basic guidance for determining risks that may require some level of compliance monitoring.[32] Texas RE will utilize the risk element development process provided in the 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.[33] Some aspects within the report correlate to the risk elements determined within the 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 in 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 analyzes generation loss events of 450 MW or greater and system event frequency deviations of +/- 0.1 Hz or greater. As such, NERC Reliability Standards related to frequency response could be utilized in compliance monitoring efforts for 2018.

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 Enterprise CMEP IP states that monitoring of a particular registered entity may include more, fewer, or different NERC Reliability Standards than those outlined in the ERO Enterprise and Regional Entity CMEP IPs. Although the ERO Enterprise CMEP IP and Regional IP identify NERC Reliability Standards and Requirements for consideration for focused compliance 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 to the BES. Therefore, a particular area of focus under a risk element does not imply that 1) the identified NERC Reliability Standard(s) fully addresses the particular risk associated with the risk element; 2) the NERC Reliability Standard(s) is only related to that specific risk element; or 3) all Requirements of a NERC Reliability Standard apply to that risk element equally.

[32] ERO Enterprise Guide for Compliance Monitoring, October 2016
[33] 2016 Assessment of Reliability Performance of the Texas RE Region, April 2017

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 NERC Reliability Standards, regardless of inclusion within the Areas of Focus described within the ERO Enterprise CMEP IP. That fact allows, as indicated by the ERO Enterprise CMEP IP, for a more in-depth review of additional requirements associated with risks beyond those shown within the ERO Enterprise CMEP 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

Table A7.1 contains the regional risk elements for focus during the 2018 based on the Regional Risk Assessment process. The table also contains Areas of Focus to identified risks that may be considered in the development of a registered entity's COP.

Table A7.1: Regional Risk Elements and Additional Areas of Focus for ERO 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., fuel type, availability, location, etc.), and voltage support capabilities in areas of the Interconnection in which voltage stability of the BES is a recognized risk. Historical events have highlighted the risks associated with voltage control and stability. Voltage stability limits are one of the driving forces for the development and continued use of Generic Transmission Limits (GTLs), a local form of SOLs in the ERCOT Interconnection. In 2016 there were 5,703 base case exceedances of GTLs for at least one Security Constrained Economic Dispatch (SCED) interval, compared to 3,269 base case exceedances in 2015.[34] 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.	TOP-001-3 R8 VAR-001-4 R1, R2, R5, R6 VAR-002-4 R1, R2, R5

[34] 2016 Assessment of Reliability Performance of the Texas RE Region, April 2017

Table A7.1: Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	The standards selected by Texas RE highlight registered entity responsibilities for providing, requesting, and ensuring that voltage support is available when needed.	
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 continues to identify 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 BES. Those risks include improper identification and mitigation of SOLs and IROLs and damage to BES equipment and facilities. The standards selected are directly tied to developing and implementing Facility Ratings for a registered entity's BES 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 processes 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	COM-001-3 R10, R11 IRO-001-4 R1 IRO-002-5 R6 IRO-008-2 R4 IRO-010-2 R1, R3 PRC-001-1.1(ii) R2 TOP-001-3 R1, R2, R13, R14 TOP-003-3 R1, R2, R3, R4, R5 TOP-006-2 R1 VAR-002-4 R3, R4, R5

Table A7.1: Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	stable electricity market. ERCOT market rules are developed by participants from all aspects of the electricity market in the ERCOT Protocols and Operating Guides, are enforced by the 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 to track.[35] Additionally, the industry determined that clarifications were needed regarding the definition of SOLs.[36] While IROL exceedances have trended downwards, there have been configuration changes within the Interconnection that have revealed new possible constraints. In 2016, approximately 13 percent of tracked events in the ERCOT Interconnection 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.	FAC-008-3 R1, R2, R3, R6 FAC-010-3 R1, R2, R3 FAC-011-3 R1, R2, R3, R5 FAC-014-2 R5 PER-005-2 R4 TOP-001-3 R8, R10, R12, R14 TOP-002-4 R1, R2, R3, R4, R5, R6 TOP-004-2 R6

[35] 2016 Assessment of Reliability Performance of the Texas RE Region, April 2017
[36] System Operating Limit Definition and Exceedance Clarification

Table A7.1: Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	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 monitoring for the pre- and post-Contingency state. Facility Rating methodology and 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 and other constraints 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.	
RAS Management	Remedial Action Schemes (RAS) 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 RAS responses include changes in demand, generation, or system configuration in an effort to alleviate the abnormal condition. Failure to properly design and implement RAS could result in the RAS not being deployed correctly, which could result in system conditions exceeding device and facility limits. Failure to maintain RAS devices could result in a misoperation of the RAS, leading to the RAS failing to operate or operating prematurely. As demonstrated by a Texas RE report, in 2016 the activation of RASs has trended upward while the arming/disarming of RASs has indicated a slight trend	IRO-002-5 R5 IRO-005-3.1a R1 IRO-010-2 R1, R3 PER-005-2 R1, R2, R3, R5, R6 PRC-001-1.1(ii) R1, R6 PRC-005-6 R1, R2 PRC-015-1 R1 PRC-017-1 R1, R2

Table A7.1: Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	downward.[37] In addition, the number of RASs in the ERCOT Interconnection has been trending downward. These trends are indicative of a possible risk associated with the management and utilization of the remaining RASs within the Interconnection. The significant change in configuration, which has—as indicated in the Texas RE report—reduced the number of RASs within the Interconnection, may be the catalyst for the increase in RAS arming. Increases in RAS arming may be indicative of possible changes in system configuration resulting in a difference in load flow. The configurations changes may be significantly different from the time a RAS was designed. While there has not been a misoperation of a RAS in the recent past, which may illustrate adequate controls regarding the maintenance and testing of RAS components beyond the Protection System components, the increase in arming of RASs is a reliability concern. The standards selected by Texas RE highlight the planning, coordination, implementation, and monitoring of RASs. The standards also highlight eh maintenance and testing requirements for RAS 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 due to the amount of load and generation in the Interconnection. 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. With significantly less load and generation	PRC-005-6 R1, R2 PRC-006-2 R1, R8, R9 PRC-008-0 R1, R2

[37] 2016 Assessment of Reliability Performance of the Texas RE Region, April 2017

Table A7.1: Regional Risk Elements and Additional Areas of Focus for ERO Risk Elements		
Regional Risk Element	**Justification**	**Associated Standard and Requirement(s)**
	than in the Eastern and Western Interconnections, the loss of generation can cause a significant drop in frequency in the ERCOT Interconnection. The change in configuration—in terms of transmission, load, 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.	
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. 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 Interconnection has areas in which voltage stability is an elevated risk. There have been historical events in which voltage stability caused instability or delayed fully returning the system to a reliable and stable state in the affected areas. The standards selected by Texas RE highlight the planning, coordination, implementation, and monitoring of the UVLS systems. The standards also highlight the maintenance and testing requirements for UVLS devices.	EOP-003-2 R2, R3, R4 PRC-005-6 R1, R2 PRC-010-2 R1, R2, R3, R4, R5, R7 PRC-011-0 R1 PRC-022-1 R1

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers risk elements, both ERO-wide and Regional, entity-specific risks, and other registered entity performance considerations, as well as internal controls, to determine how a RE will monitor a registered entity's compliance with the NERC Reliability Standards. This section includes regional risk-based CMEP activities occurring during the 2018 implementation year.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists planned Audits for registered entities during the 2018 implementation year. The 2018 Compliance Audit Plan, located on the RE's website (www.texasre.org), details the registered entity's NCR, registered entity's name, and scope of monitoring for the NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2018 Compliance Audit Plan for Texas RE is located here: Annual Audit Plan for Compliance Audits for 2018. Throughout the implementation year, the RE will may make updates to the 2018 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

The RE conducts Spot Checks based on a registered entity's COP, or at RE discretion at any time. The RE may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, and Periodic Data Submittals, or to assess compliance with NERC Reliability Standards. The RE will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a Spot Check.

Self-Certifications

The RE determines Self-Certifications based on a registered entity's COP or based on regional risks and other considerations. The RE will follow the ROP for notifying registered entities of any Self-Certifications, ensuring advanced noticed according to the ROP.

Texas RE does not have any planned Regional Self-Certifications in 2018. Texas RE will utilize Self-Certifications on individual entities as a result of the individual registered entity's inherent risk assessment and compliance oversight planning.

Periodic Data Submittals

Some NERC Reliability Standards require data submittals on a monthly, quarterly, or annual basis. The RE follows the 2018 ERO Enterprise Periodic Data Submittals Schedule posted on the NERC website. NERC and the REs may also request data or information under Sections 800 or 1600 of the ROP; these data requests are not included on this schedule.

Compliance Outreach

Table A7.2: Compliance Outreach Activities

Outreach Activity	Anticipated Date
Spring Compliance Workshop	Spring 2018
Compliance 101	Summer 2018
Fall Compliance Workshop	Fall 2018
Talk with Texas RE	Projected Monthly (subject to change)
Texas *RE*view Newsletter	Projected Monthly

Appendix A8: Western Electricity Coordinating Council (WECC) 2018 CMEP Implementation Plan

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

Compliance Monitoring and Enforcement

CMEP IP Highlights and Material Changes

WECC will follow and perform the ERO Risk-Based Compliance Oversight Framework described in the ERO Enterprise CMEP IP. WECC monitors FERC and NERC activities, system events, and events in the WECC Region. Based on these monitoring activities, WECC may modify its CMEP IP throughout the year to address and mitigate situational awareness and reliability issues as they arise. The 2018 ERO Enterprise CMEP IP identifies several Risk Elements and areas of focus that provide a starting point for WECC's risk analysis and COP development. However, the 2018 ERO Enterprise CMEP IP recognizes that it does not include the complete set of the risks that may affect the 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.

WECC performed its Regional Risk Assessment, which identified risks within the WECC Region. In 2018, WECC may monitor the NERC Reliability Standards (Standards) and Requirements associated with these risks, which are referred to as the 2018 WECC Risk Elements. WECC 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 IRAs and historical performance considerations.

Other Regional Key Initiatives & Activities

Risk-Based Enforcement

WECC will continue to use a risk-based enforcement approach consistent with the ERO Enterprise. Specifically, WECC will exercise enforcement judgment 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 non-compliances. However, WECC will continue to use the FFT disposition method for moderate-risk issues or minimal-risk issues that WECC 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 WECC grants to a registered entity based on the entity's demonstrated ability to identify, assess and correct non-compliances, in addition to other factors. Case-by-case compliance exceptions are based on the facts and circumstances of a particular non-compliance. Self-logging privileges allow the presumption of compliance exception treatment for self-identified minimal-risk issues.

Self-Logging

Self-logging allows qualified registered entities to keep a log of minimal-risk non-compliances that WECC periodically checks in lieu of submitting individual self-reports and corresponding mitigation plans for each non-compliance. For each logged non-compliance, 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 WECC for review and approval every three months. WECC checks to ensure the non-compliance is sufficiently described, the minimal-risk determination is justified and reasonable, and the mitigation is appropriate and adequate. After WECC approves the log entries, they are processed as compliance exceptions.

Logging privileges are awarded based on WECC's historical interactions with the registered entity, combined with WECC's evaluation of the registered entity's current ability to identify, assess, and correct non-compliances (an evaluation that is scaled based on the risk posed by that registered entity). With respect to historical interactions, WECC will consider the registered entity's

1. compliance history and level of cooperation in prior compliance matters;
2. history of self-assessment, self-reporting, and timely and thorough mitigation; and
3. quality, comprehensiveness, and execution of its internal compliance program.

For most registered entities, this is information that is already available to WECC.

A registered entity's current practices to identify, assess, and correct non-compliances are important to the analysis because self-logging relies on the entity's ability to properly arrive at its minimal risk determinations. In a traditional self-reported enforcement action, WECC does its own risk analysis and makes its decision about how to treat the violation based on that analysis. WECC does not allow compliance exception treatment for minimal-risk issues identified through self-logging without adequate assurance that the registered entity has processes in place to identify, assess, and correct non-compliances. In some circumstances, this information may already be available to WECC through prior dealings with a registered entity. If it is not already available, WECC may request that information through interviews and documentation.

One way to provide that information and potentially reduce audit scope is to have WECC's Compliance Risk Analysis Team conduct an internal controls evaluation focused on risk management. However, an internal controls evaluation is not required for WECC to award self-logging privileges.

Regional Risk Assessment Process and Results

WECC's Entity Oversight Department performs an annual Regional Risk Assessment that contributes to the development of this appendix to the ERO Enterprise CMEP IP. The collection of data and subsequent assessment is completed to determine previously identified and emerging risks that pose the greatest potential impact to the reliability of the Western Interconnection. WECC's Regional Risk Assessment includes a review of data including, but not limited to, the following:

- Risks currently identified in the ERO Enterprise CMEP IP
- Data and results of IRAs
- Data and results of residual risk following controls evaluations
- Trends identified with Regional non-compliances and corresponding causes
- Situational awareness, event, and misoperations reports
- The State of the Interconnection Report for the Western Interconnection
- NERC Alerts and FERC Orders
- Professional judgment of WECC Entity Oversight personnel

The goal of the assessment is to improve the awareness of the Entity Oversight Department personnel with respect to the Regional operational risks, the ERO-identified risks, and risks associated with instances of documented non-compliance. The information will be used by the WECC Entity Oversight Team for assessing risk associated to a non-compliance while developing a COP.

The results of the assessment will include NERC Reliability Standards and Requirements, to be monitored by WECC's Entity Oversight Department to address the risks (e.g., standards, compliance monitoring activities, or any other

Regional oversight activities). The risks and requirements from the results of the assessment will be categorized into the Risk Elements identified in the ERO Enterprise CMEP IP and additional Regional Risk Elements that have been determined necessary to supplement the ERO-identified Risk Elements.

WECC may include additional detail on WECC Risk Elements and their associated NERC Standards and Requirements in the 2018 registered entity-specific COPs. The Regional Risk Assessment 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—WECC will update the Regional Risk Assessment to keep current with potential issues, threats, and risks.

WECC reviews the potential risks to the reliability of the BPS posed by an individual registered entity by using ERO IRA guidance and the associated internal IRA procedure to perform the registered entity IRA. The results of Regional Risk Assessment further influence the COP development process for each registered entity.

Based on the results of the Regional Risk Assessment, WECC will exclude the Areas of Focus in Table A8.1 from the WECC 2018 CMEP IP:

Table A8.1: Regional Areas of Focus - Exclusions

Exclusion ERO Risk Elements	Justification	Additional Standard and Requirement(s)
Planning and System Analysis	The WECC Regional Risk Assessment has identified that VAR-001-4 Requirement 5 is not applicable to the registered entities in Western Interconnection, due to the regional variance.	VAR-001-4.1 R5

Regional Risk Elements and Areas of Focus

The 2017 WECC Regional Risk Assessment identified the following 2018 WECC Risk Elements. These elements align with the 2018 ERO Risk Elements and therefore constitute Expanded ERO Risk Elements:

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

Table A8.2 contains the Regional Risk Elements that WECC identified during the Regional Risk Assessment process. During its review, WECC identified associated NERC Reliability Standards and Requirements for increased compliance monitoring focus in 2018. Thus, WECC justified their inclusion during the Regional Risk Assessment.

In Table A8.2, WECC provides *additional justifications where applicable.* These NERC Reliability Standards and Requirements will be considered as part of the COP development and may or may not be included in the registered entity-specific COP.

Table A8.2: Additional Areas of Focus for ERO Risk Elements

Expanded ERO Risk Elements	Justification	Additional Standards and Requirement(s)
Human Performance	There are 245 registered entities in the Western Interconnection that have the GOP Function. COM-002-4 R3 is a new Requirement for the DP and GOP Functions. Therefore, the performance of most entities with respect to R3 is not known and proper three-part communication is essential to the Reliable operation of the Western Interconnection. Of the COM-002-4 non-compliance issues in the WECC Region, 44 percent have occurred with R3.	COM-002 R3
Maintenance and Management of BPS Assets	The WECC Regional Risk Assessment has identified that Risk Factors assessed in its IRA process that are associated with the Maintenance and Management of BPS Assets Area of Focus have been rated as medium or high 44 percent of the time. Application of this Requirement for registered entitles in the Western Interconnection indicates a high risk to reliability for the associated Area of Focus.	FAC-501-WECC-1 R3
Planning and System Analysis	The WECC Regional Risk Assessment has identified that Risk Factors in its IRA process that are associated with the Planning and System Analysis Area of Focus have been rated medium or high 46 percent of the time. In the WECC Region, the Coordinated Off-Nominal Frequency Load Shedding and Restoration Plan is based on the BA Area load. The BA, or its agent(s), are responsible to coordinate with UFLS entities in its area to assure all requirements of the coordinated plan are met. This Requirement is applicable to PCs. Therefore, the gap that exists between planning for a UFLS event and the execution of the devices between BAs and PCs presents a concern that each PC shall participate in a joint Regional review.	PRC-006-2 DB1
Protection System Failures	The WECC Regional Risk Assessment has identified that Risk Factors assessed in its IRA process that are associated with the Protection System Failures Area of Focus, have been rated medium or high 63 percent of the time. Monitoring of the Requirement will ensure that the entity has analyzed transmission and generation Protection System and RAS misoperations on Major WECC Transmission Paths and RAS.	PRC-004-WECC-2 R1

Regional Compliance Monitoring Plan

The ERO Enterprise follows a Risk-Based Compliance Monitoring Framework that considers: 1) Risk Elements, both ERO-wide and Regional; 2) entity-specific risks; and 3) other registered entity performance considerations, as well as internal controls. Using this information, the ERO Enterprise determines how a Regional Entity will monitor a

registered entity's compliance with the NERC Reliability Standards. This section includes Regional risk-based CMEP activities occurring during the 2018 implementation year.

Inherent Risk Assessments

In 2018, WECC will continue to use the ERO Enterprise Guide for Compliance Monitoring to determine the inherent risk posed by an entity to reliability of the Interconnection. WECC will also review again the inherent risk of BA/TOPs and the RC that were assessed using different risk factors. WECC plans on completing IRAs for all registered entities within WECC by the end of 2018.

Compliance Oversight Plans

In 2018, WECC will continue to use the ERO Enterprise Guide for Compliance Monitoring to determine the frequency, scope, and CMEP tool to be used for compliance monitoring activities. WECC will continue its focus on identifying, prioritizing, and addressing risks to the BES by analyzing several performance criteria specific to entities' characteristics and past performance, and Regional risks associated with the Areas of Focus identified in Table A8.2 of WECC's CMEP IP. This will further allow WECC to focus resources where they are most needed. WECC considers a COP to be a living document and will continue to review and update the COP based on these performance criteria. WECC plans on developing COPs for all registered entities within WECC by the end of 2018.

Compliance Audits

The Regional Compliance Monitoring Plan includes the 2018 Compliance Audit Plan that lists all planned Audits for registered entities during the 2018 implementation year. The 2018 Compliance Audit Plan, located on WECC's website, details the registered entity's NCR ID, name, and scope of monitoring for NERC Reliability Standards (i.e., Operations and Planning and/or Critical Infrastructure Protection).

The 2018 Compliance Audit Plan for WECC is located here: WECC website. Throughout the implementation year, WECC will may make updates to the 2018 Compliance Audit Plan based on risk-based compliance monitoring activities.

Spot Checks

WECC conducts Spot Checks based on a registered entity's COP or at its discretion at any time. WECC may conduct a Spot Check in response to events, to support a registered entity's Self-Certification, Self-Report, or Periodic Data Submittal(s), or to assess compliance with NERC Reliability Standards. WECC will follow the process outlined in Appendix 4C of the ROP to initiate and conduct a Spot Check.

Self-Certifications

WECC determines Self-Certifications based on a registered entity's COP or on Regional risks and other considerations. WECC will provide advanced notice of Self-Certifications to registered entities in accordance with the ROP. The Self-Certification schedule is located on WECC's website.

WECC will perform guided Self-Certifications as needed throughout 2018. The guided Self-Certifications for a registered entity will be based on 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 issues and may require the registered entity to submit substantiating evidence to support its determination.

Table A8.3: WECC 2018 Self-Certification Schedule

Functions	Entity Notification Date	Submittal Window Opens	Submittal Window Closes	Reporting Form	Submittal Method

BA, DP, FRSG, GO, GOP, PA/ PC, RC, RSG, RP, TO, TOP, TP, TSP, DP UFLS-Only	December 15, 2018	January 1, 2019	March 1, 2019	Self-Certification Menu in webCDMS	webCDMS, Compliance, Self-Certification

Periodic Data Submittals

Some NERC Reliability Standards require data submittals monthly, quarterly, or annually. WECC will follow the 2018 ERO Enterprise Periodic Data Submittals Schedule and the WECC 2018 Periodic Data Submittal schedules located on WECC's website.

Compliance Outreach

Compliance Workshop

The Compliance Workshop provides in-depth, in-person, detailed training and education through structured lecture and presentation, panels of experts, and interactive dialogue in an open forum, with direct question and answer sessions and invaluable networking opportunities. Workshops cover the entire compliance sphere, focusing on the attendees' and industry's issues. These meetings provide direct access to the WECC Entity Oversight management team, staff, and SMEs. Participants may also attend telephonically or via video webinar. The Compliance Workshop schedule is posted on WECC's website.

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 current 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.

Table A8.4: Compliance Outreach Activities

Outreach Activity	Anticipated Date
WECC Open Webinar	Third Thursday of most months
Compliance Workshop	March 27-29, 2018 Boise, ID October 23-25, 2018 San Diego, CA

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 potentially implicated by the causes and contributing factors of the event.
3. After reviewing the facts and circumstances of the event, develop conclusions applicable to relevant NERC Reliability Standards and Requirements (see Step 2 above).
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