NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2020 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 2.0

November 2019

RELIABILITY | RESILIENCE | SECURITY




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

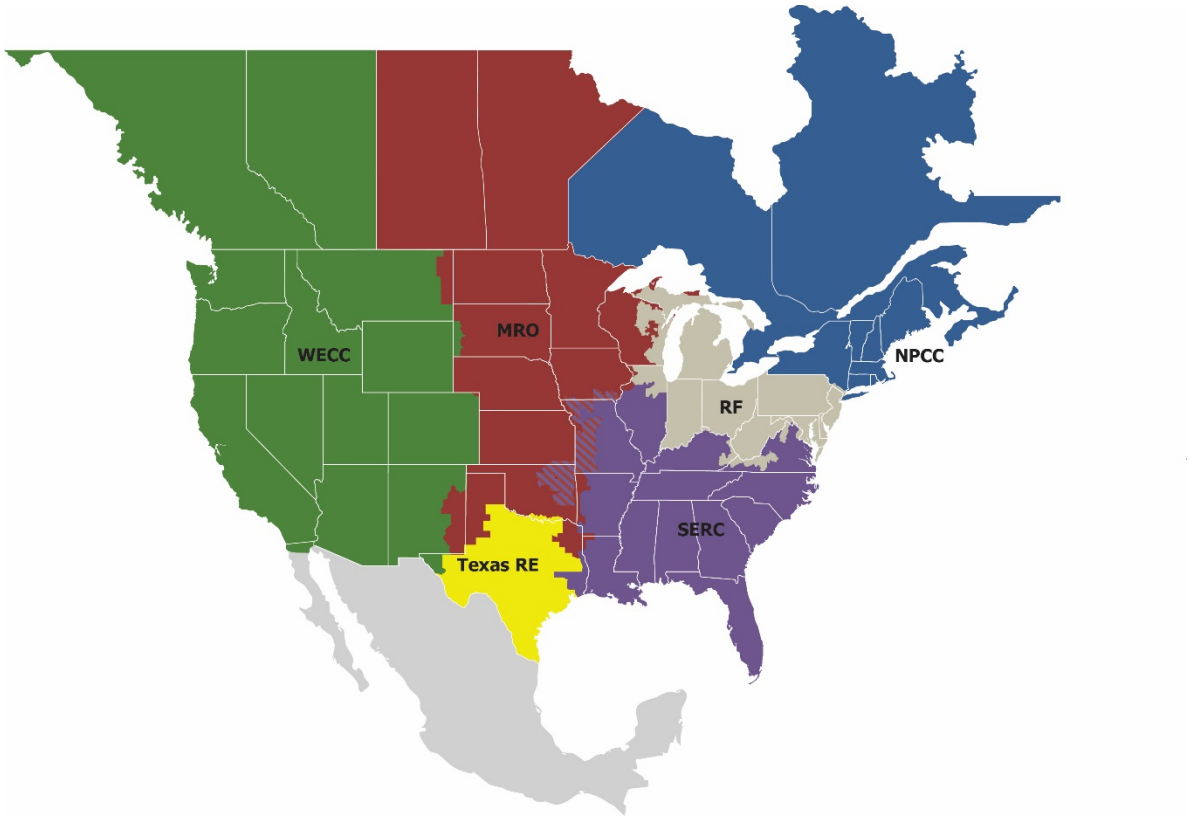
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Revision History

Version	Date	Revision Detail
Version 1.0	September 2019	• Release of the 2020 ERO CMEP Implementation Plan.
Version 2.0	November 2019	• Added links to Regional Monitoring Schedules • Added link to Periodic Data Submittal schedules • Updated risk element descriptions based on 2019 ERO Reliability Risk Priorities Report

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 development of an annual CMEP IP.[2]

The ERO Enterprise is pleased to release an enhanced, easier to use CMEP IP for this year. Collectively, NERC and each RE have worked collaboratively throughout this IP's development to streamline the ROP's timing and risk assessment processes into one cohesive narrative, compared to a main IP with several regional appendices as in years past. By streamlining the development in this manner, the ERO Enterprise believes that it is also more effectively and efficiently fulfilling the timing and risk assessment obligations of the CMEP IP, which will also enhance efforts to modify and adjust going forward.

Through this enhancement, the ERO Enterprise will address areas where there may be specific regional considerations in the main risk element description itself. The ERO Enterprise believes that this will make the IP both more user-friendly and relevant to registered entities. Specifically, the IP represents the ERO Enterprise's high-level priorities for its CMEP. While the ERO Enterprise will determine individual monitoring decisions for each registered entity based on its unique characteristics, registered entities should consider the risk elements and their associated areas of focus as they evaluate opportunities and their own prioritization to enhance internal controls and compliance operations focus.

Monitoring Schedules

Please find the following links provided by the Regional Entities to their planned monitoring schedules:

- MRO: MRO Audit Schedules
- NPCC: NPCC Audit Schedules
- ReliabilityFirst: ReliabilityFirst Compliance Monitoring Page (see Schedules)
- SERC: SERC 2020 Compliance Audit Plan
- Texas RE: Texas RE 2020 Annual Audit Plan
- WECC: WECC Draft 2020 US Audit Schedule

[1] The ERO Enterprise comprised of NERC and the six Regional Entities, which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the ERO's statutory obligations to assure the reliability of the North American BPS.

[2] NERC ROP, Appendix 4C Section 4.0 (Annual Implementation Plans).

Periodic Data Submittals

The Compliance Enforcement Authority (CEA) requires Periodic Data Submittals in accordance with the schedule stated in the applicable Reliability Standards, as established by the CEA, or as-needed, in accordance with the NERC Rules of Procedure (RoP), Appendix 4C Section 3.6.

MRO[3] and WECC[4] have posted their schedules for periodic data submittals. The other four Regional Entities use the periodic data submittal schedule posted by NERC here:
NERC Compliance Resource Documents

[3] MRO Self Certifications

[4] WECC Draft 2020 Periodic Data Submittal and Self-Certification Schedule

2020 ERO Enterprise Risk Elements

Process for Risk Elements and Associated Areas of Focus

The ERO Enterprise uses the ERO Enterprise Risk-based Compliance Monitoring Framework (Framework) to identify both ERO-Enterprise-wide risks to the reliability of the BPS and mitigating factors that may reduce or eliminate a given reliability risk. The ERO Enterprise accomplishes this by using the risk element development process.[5] As such, the ERO Enterprise identifies risk elements using data including, but not limited to: compliance findings; event analysis experience; data analysis; and the expert judgment of ERO Enterprise staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee). Reviewed publications include the Reliability Issues Steering Committee's (RISC) report,[6] The State of Reliability Report, [7] the Long-Term Reliability Assessment, publications from the RISC, special assessments, the ERO Enterprise Strategic Plan, and ERO Event Analysis Process insights. The ERO Enterprise uses these risk elements to identify and to prioritize interconnection and continent-wide risks to the reliability of the BPS. These identified risks are used to focus compliance monitoring and enforcement activities.

The ERO Enterprise reviewed and reassessed the 2019 risk elements to determine applicability for 2020. Although the IP identifies NERC Reliability Standards and Requirements to be considered for focused CMEP activities, the ERO Enterprise recognizes by using the Framework and other risk-based processes that REs will develop an informed list of NERC Reliability Standards and Requirements specific to the risk a registered entity poses for any monitoring activities. Notably, the implementation plan is not intended to be a representation of just "important" Reliability Standards requirements; rather, it is intended to reflect the ERO Enterprise's prioritization within its CMEP based on its inputs and to communicate to registered entities to bring collective focus within their operations to address each prioritized risk.

Impact of Risk Elements

The REs evaluate the relevancy of the risk elements to the entity's facts and circumstances as they plan CMEP activities throughout the year. For a given registered entity, requirements other than those in the CMEP IP may be more relevant to assist mitigating the risk, or the risk may not apply to the entity at all. Thus, depending on regional distinctions or registered entity differences, focus will be tailored as needed.

The 2020 risk elements are included in Table 1 below and reflect a maturation of the risk-based approach to compliance monitoring. As the ERO Enterprise and industry continue to become more knowledgeable about the risks that require control emphasis or mitigation, risk elements will focus more on discrete risks. These discrete risks provide focus for measuring current state and validating registered entity progress. By tracking improvements, industry and the ERO Enterprise can justify focusing on different risks in the future.

[5] Appendix C, ERO Enterprise Guide for Compliance Monitoring; October 2016

[6] ERO Reliability Risk Priorities; February 2018

[7] NERC State of Reliability 2018, available at https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_2018_SOR_06202018_Final.pdf

Compliance monitoring is not the only tool available to address the risks identified. CMEP staff may assist in various forms of outreach with industry to encourage best practices to achieve the common goal of mitigating risk to the BPS.[8] Enforcement may consider these risks when assessing risk for possible noncompliance, assisting with mitigation plans, or assessing penalties.

Table 1: Comparison of 2019 Risk Elements and 2020 Risk Elements

2019 Risk Elements	2020 Risk Elements
Improper Management of Employee and Insider Access	Management of Access and Access Controls
Insufficient Long-Term Planning Due to Inadequate Models	Insufficient Long-Term and Operations Planning Due to Inadequate Models
Insufficient Operational Planning Due to Inadequate Models	
Spare Equipment with Extended Lead Time	Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages	Inadequate Real-time Analysis During Tool and Data Outages
Improper Determination of Misoperations	Improper Determination of Misoperations
Inhibited Ability to Ride Through Events	Gaps in Program Execution
Gaps in Program Execution	Texas RE: Resource Adequacy

Management of Access and Access Controls

The protection of critical infrastructure remains an area of significant importance. This risk element establishes a focus on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.[9] Regardless of the sophistication of a security system, there is potential for human error. Compliance monitoring should seek to understand how entities manage the risk of access, including insider threat and remote access, and the complexity of the tasks the individuals perform. If security has increased the difficulty in performing personnel's normal tasks, personnel will look for ways to circumvent the security to make it easier to perform their job. On the other hand, when an entity replaces complex tasks with automation, focus should be on:

[8] For example, in 2019, the ERO Enterprise noted in its 2019 CMEP IP that it may engage in targeted efforts to understand entities implementation of specific, newer aspects of IRO-008 and TOP-001. NERC, RE, and FERC staff worked in 2019 to better understand the strategies and techniques used by entities to perform Real-time Assessments (RTAs) during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the Regional Entities (REs) began collaborating with a small number of entities to focus on the practices and controls to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001). Aggregated information on potential industry best practices and concerns will be outlined in a public report after completion of the activity, which is expected in 2020.

[9] ERO Reliability Risk Priorities; February 2018

1) whether the automation was correctly configured; 2) controls to ensure the automation is operating as intended; and 3) how access, the ability to obtain and use, is implemented.

Harvesting credentials and exploiting physical and logical access of authorized users of BES facilities and Cyber Systems (BCSs) pose a major risk to systems that monitor and control the BES. With the target being users, privileged or non-privileged, who have authorized unescorted physical access and/or various levels of access to critical elements of the BES, the risk becomes elevated. By actively and covertly employing social engineering techniques and phishing emails, attackers may deceive authorized users to harvest credentials and gain unauthorized access.[10]

BES Cyber Systems possibly compromised by unauthorized access using another's credentials is a major business, compliance, and security risk to systems that monitor and control the BES. 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. Examples of this includes systems designed to run autonomously with minimal human interaction and other mission-critical applications that perform supervisory control that, if misused, could result in serious reliability issues. Additionally, remote devices susceptible to compromise that remotely access a Cyber Asset can serve as a gateway for cyber-criminals to attack networks.

Additionally, malicious code penetration attempts on both the Information Technology (IT) and Operational Technology (OT) systems are on the rise. This Area of Focus brings industry's attention to potentially reduce the attack vectors of hackers, malicious code exploitation, and ransomware penetration.

Mitigation of the identified area's risks is through awareness and technical controls. Entities need to enhance security awareness to include specific topics on social engineering and insider threat. Entities can proactively reduce the insider and external threats by implementing detection and monitoring tools as technical controls. Further, a formalized insider threat management program in place can vastly reduce the associated risk.

[10] US-CERT TA18-074A

Areas of Focus

Table 2: Management of Access and Access Controls			
Standard	**Requirement**	**Entities for Attention**	**Asset Types**
CIP-003-7 CIP-003-8 (eff. 4/1/2020)	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Back up Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-004-6	R4, R5	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-005-5 CIP-005-6 (eff. 7/1/2020)	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-006-6	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-007-6	R1, R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-010-2 CIP-010-3 (eff. 7/1/2020)	R1, R4	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations

CIP-011-2	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-013-1 (eff. 7/1/2020)	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	

Insufficient Long-Term and Operations Planning Due to Inadequate Models

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 inverter-based resources and variable energy resources, changes in load characteristics, increasing dependence on natural gas deliverability for gas-fired generation, increasing uncertainty in nuclear generation retirements, and essential reliability services). NERC's annual Long-Term Reliability Assessment[11] forms the basis of NERC's assessment of emerging reliability issues. The ERO continues to raise awareness on inverter-based resource performance through NERC alerts[12] and industry outreach. Compliance monitoring should seek to understand how entities manage the risk of planning in this changing environment.

Insufficient long-term planning can lead to increased risks to reliability. Adequately modeled planning cases become increasingly critical as a changing resource mix, deployment of new technologies, etc., affect the risk to BPS reliability. For instance, the models should reflect if the power electronic controls of utility-scale inverter-based resources, such as PV resources, give these resources the ability to provide both real and reactive power. As stated in the 2018 RISC report,[13] since the rate of change of the resource mix is increasing, planners will place more emphasis on interconnection-wide studies that require improvement to and integration of regional models. In addition, enhancements to models will be needed to support probabilistic analysis to accommodate the energy limitations of resource additions (such as variable renewable resources). Resource adequacy must look beyond the calculation of reserve margins that assume actual capacity available during peak hours.

Insufficient operational planning can lead to increased risks to reliability. More comprehensive dynamic load models will be needed to sufficiently incorporate behind-the-meter generation and distributed load resources such as demand-side management programs. One of the ways in which the industry can better understand the system is by monitoring load characteristics and the changing nature of load due to Distributed Energy Resources (DER). The NERC Load Modeling Task Force developed a reliability guideline that provides Transmission Planners (TPs) and

[11] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2018_12202018.pdf

[12] https://www.nerc.com/news/Documents/Inverter%20Alert%20Announcement.pdf

[13] ERO Reliability Risk Priorities; February 2018

Transmission Owners (TOs) with insights into end-use load behaviors and how to capture them in the composition of dynamic load models.[14]

In order to achieve performance expected by the planning models, generating plant protection schemes and their settings should be coordinated with transmission protection, control systems, and system conditions to minimize unnecessary trips of generation during system disturbances.[15]

Planning models are reliant on correct Facility Ratings. See the "Gaps in Program Execution" risk element later in this document for more information.

Additional studies have similarly shown a need to more accurately understand and model inverter-based resource characteristics. NERC has identified adverse characteristics of inverter-based resources in two separate Alerts.[16,17] With the recent and expected increases of both utility-scale solar resources and distributed generation, the causes of a sudden reduction in power output from utility-scale power inverters needs to be widely communicated and addressed by the industry. Entities with increasing inverter-based resources should be aware and addressing this within their models.[18]

Areas of Focus

Table 3: Insufficient Long-Term and Operations Planning Due to Inadequate Models

Standard	Requirements	Entities for Attention	Rationale
MOD-033-1	R1, R2	Planning Coordinator Reliability Coordinator Transmission Operator	Validating planning power flow models.
PRC-023-4	R1, R2, R6	Transmission Owner Generator Owner Planning Coordinator	Ensure protective relay settings do not limit transmission loadability.

[14] NERC Modeling Improvements Initiative Update; May 2018

[15] Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings; June 2017

[16] Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings - II; May 2018

[17] NERC Modeling Notification: Recommended Practices for Modeling Momentary Cessation Distribution; April 2018

[18] Considerations for Power Plant and Transmission System Protection Coordination, July 2015

PRC-024-2	R1, R2	Generator Owner	Ensure resources stay available during applicable voltage and frequency excursions, especially inverter-based resources.
TPL-001-4	R1	Planning Coordinator Transmission Planner	Ensure accurate System models.

Loss of Major Transmission Equipment with Extended Lead Times

There are several scenarios that can damage expensive, long-lead time transmission equipment which can reduce contingency margins while industry implements emergency procedures and works towards replacing the equipment. These reasons include:

- aging infrastructure coupled with less than adequate maintenance
- failure of large power transformers due to the effects of a Geomagnetic disturbance, wild fires, or other weather-related effect
- any type of intentional (or unintentional) physical or cyber-security breach, including the impacts of an EMP

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.

An entity's awareness of which of its Facilities have extended replacement lead times can affect real-time operations. In some cases, pre-emptive actions may be needed to protect identified major transmission equipment with extended lead times. As noted in the posted draft 2019 RISC Report: "Wild Fires can be a direct threat to BES equipment. Pre-emptive actions must be taken to de-energize equipment without causing additional cascading effects in areas where wild fire risk is significant."[19]

Spare equipment strategy is an important aspect of restoration and recovery. The strategy should encompass identifying critical spare equipment as part of a national or regional inventory. For example, as part of the changing resource mix supplying power to the BPS, many Blackstart units are being retired; remaining Blackstart units become more critical to ensure proper and timely system recovery. The strategy should also account for the transportation and logistics requirements for replacing critical assets. An improved spare equipment strategy or plan will lead to better contingency planning and possibly faster response times for restoration and recovery. A spare equipment strategy can help strengthen the resiliency for responding to potential physical threats and vulnerabilities.[20]

[19] DRAFT 2019 RISC Report

[20] CIP-014-2 Guidelines and Technical Basis, Requirement R5

Areas of Focus

Table 4: Loss of Major Transmission Equipment with Extended Lead Times			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
EOP-005-3	R7	Transmission Operator	Assess whether unavailability of Blackstart units and their associated systems, including Blackstart paths have been considered in the entity's spare equipment strategy.
TPL-001-4	R2.1.5	Planning Coordinator Transmission Planner	Ensure that unavailability of major Transmission equipment has been considered in the entity's spare equipment strategy.

Inadequate Real-time Analysis during Tool and Data Outages

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.

Specifically, entities are to be encouraged to have realistic plans to continue real-time analysis during outages of tools, loss of data, or both. The 2018 RISC report[21] identifies that loss of situational awareness can be a precursor or contributor to a BPS event. This risk element is made more important in situations where planning models may not keep pace with increasing BPS complexity and accurately reflect area-specific dependencies on inverters, natural gas, or other items identified in the other 2020 risk element "Insufficient Long-Term and Operations Planning Due to Inadequate Models". Forecasting BPS resource requirements to meet customer demand is becoming increasingly difficult due to the penetration of DER which can mask the customer's electric energy use and the operating characteristics of distributed resources without sufficient visibility.

Registered entities should be able to clearly demonstrate their plan and the capability and feasibility of the entities skilled workforce to implement the plan within a reasonable time frame. Compliance monitoring should include a keen eye on events and the human evaluation rather than simply looking at RTCA scans. RTCA is a tool to help achieve the intent of these requirements, but RTA is the human evaluation of computer generated results and other relevant inputs. While the two are linked in this process, simply having RTCA running in the background does not constitute an assessment of the system (i.e., an RTA).

This risk element will be reevaluated pending the results of ongoing activities. The ERO Enterprise and FERC staff are seeking to better understand the strategies and techniques used by entities to perform RTAs during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the Regional Entities (REs) are collaborating with a small number of entities in 2019 to focus on the practices and controls to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001).

[21] ERO Reliability Risk Priorities; February 2018

Aggregated information on potential industry best practices and concerns will be outlined in a public report after completion of the activity.

Areas of Focus

Table 5: Inadequate Real-time Analysis during Tool and Data Outages			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
IRO-008-2	R4	Reliability Coordinator	Ensuring situational awareness is maintained regardless of RTCA status
TOP-001-4	R13	Transmission Operator	Ensuring situational awareness is maintained regardless of RTCA status

Improper Determination of Misoperations

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),[22] the August 14, 2003 Blackout (see recommendation 21),[23] and the Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015 (see recommendation 2).[24]

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 should not 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.

The 2018 RISC report[25] includes a key point that the ERO Enterprise, the impacted organizations, and the respective forums and trade organizations should perform post-event reviews to capture lessons learned and how to reduce the impact of future events. These reviews will be incomplete if not every event is noticed because the relay operations were not reviewed by qualified personnel. The report also identifies the risk posed by the increasing complexity in protection and control systems, further emphasizing the importance of a skilled workforce analyzing events and relay operations. Understanding how an entity uses controls can help promote best practices in this area.

Areas of Focus

Table 6: Improper Determination of Misoperations			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
PRC-004-5(i)*	R1, R3	Generator Owner Transmission Owner	Ensure proper analysis of protection system operations.

[22] See Arizona-Southern California Outages on September 8, 2011

[23] See Final Report on the August 14, 2003 Blackout

[24] See Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015

[25] ERO Reliability Risk Priorities; February 2018

Gaps in Program Execution

The ERO Enterprise has observed an increase in FAC-003-3 R2 violations resulting in vegetation contacts. These violations result from vegetation management programs that have less than adequate procedures to address identified problems or that fail to adapt to changing conditions, e.g., increased precipitation that accelerates vegetation growth.[26]

Change management weaknesses have also led to significant violations related to Facility Ratings and maintenance of Protection System devices. Some registered entities have Facility Ratings based on inaccurate equipment inventories, or ratings are not being updated during projects or following severe weather. Where records are not kept up to date, inaccurate models and damaged equipment can result. Failing to keep accurate inventories of equipment, following asset transfers, addition of new equipment, or mergers and acquisitions, is also resulting in incomplete Protection System Maintenance and Testing Programs that jeopardize the functionality of the equipment to respond to faults or disruptions on the electric system.

Areas of Focus

Table 7: Gaps in Program Execution

Standard	Requirements	Entities for Attention	Rationale
CIP-002-5.1a	R1, R2	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator	Ensuring entities maintain complex programs which handle large amounts of data, e.g., accurate inventories of equipment, following asset transfers, addition of new equipment, etc.
CIP-010-2 CIP-010-3 (eff. 7/1/2020)	RI	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator	
FAC-003-4	R1, R2, R3, R6, R7	Generator Owner Transmission Owner	
FAC-008-3	R6	Generator Owner Transmission Owner	
PRC-005-6	R3	Generator Owner Transmission Owner	

Texas RE: Resource Adequacy

This risk element is primarily focused on the Texas interconnection, although facts and circumstances of entities elsewhere may warrant similar focus. This risk element aims ensuring the available resources are appropriately managing frequency control and voltage control aspects in the Interconnection. 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 have been changes in the ERCOT Interconnection that have facilitated the use of more dynamic and static reactive devices in more areas. Additionally, there are several load pockets where the management of reactive resources plays a significant role in

[26] *See* Notices of Penalty filed June 27, 2019 in FERC Docket No. NP19-13-000, August 30, 2018 in FERC Docket No. NP18-23-000, and May 31, 2018 in FERC Docket Nos. NP18-11-000, NP18-12-000, and NP18-13-000

ensuring reliability. While frequency control metrics are being maintained at a high level, the shift in resource mix warrants appropriate compliance monitoring. The impact on system inertia is a risk as the resource mix continues to evolve. The load growth coupled with record breaking wind penetration puts an emphasis on managing the frequency before, during, and after events. Resources should have appropriate controls in place to support reliable operations as the resource mix within this Interconnection continues to change. All entities should have proper plans in place to act and react to operational risks.

Areas of Focus

Table 8: Texas RE: Resource Adequacy

Standard	Requirements	Entities for Attention	Rationale
BAL-001-TRE-1	R9, R10	Generator Owner	(Where applicable) Ensure generating resources achieve expected frequency response.
PRC-024-2	R2	Generator Owner	Ensure proper availability of generating resources.
VAR-002-4.1	R2	Generator Owner	Ensure generating resources maintain their given generator voltage or Reactive Power schedule.