NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2022 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 1.0

October 2021

RELIABILITY | RESILIENCE | SECURITY




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

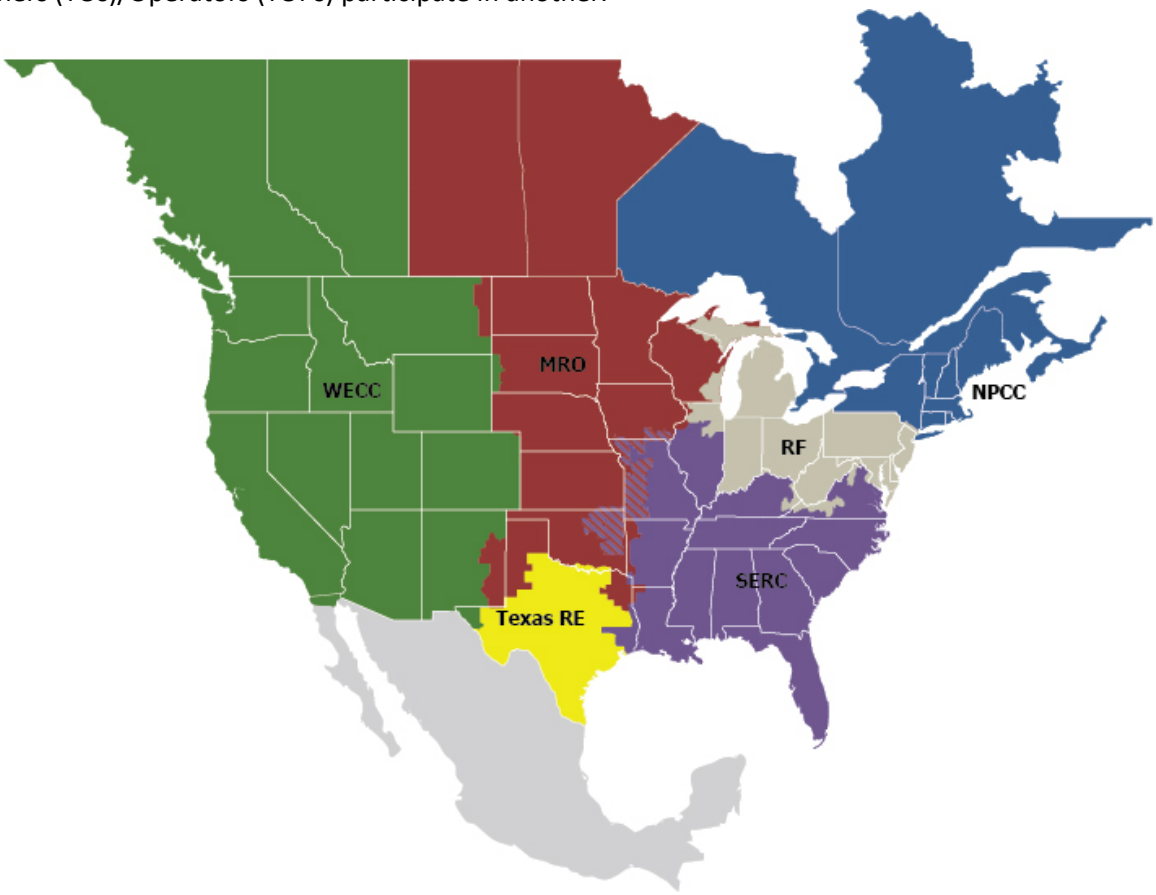
Table of Contents

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 made up of 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 RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



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

Revision History

Version	Date	Revision Detail
Version 1.0	October 2021	• Release of the 2022 ERO CMEP Implementation Plan.

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 the 2022 CMEP IP describing the risks that will be priorities for the ERO Enterprise's CMEP activities in 2022. Collectively, NERC and each Regional Entity (RE) have worked collaboratively throughout this CMEP IP's development to evaluate reports of NERC committees (especially the Reliability Issues Steering Committee [RISC]), ERO Enterprise analysis of events, and NERC reliability assessments to identify the existing and emerging risks to reliable and secure operations.

This strategic CMEP IP highlights the focus of our monitoring and enforcement efforts in 2022 on the risk elements identified within. The CMEP IP gives guidance to the employees of the ERO Enterprise involved with monitoring and enforcement, and through public posting informs the ongoing conversations with industry about the risks we all seek to mitigate. The risk elements described herein are all developed with the four risks designated "manage" and the four risk profiles, all identified in the 2021 RISC ERO Reliability Risk Priorities Report.[3] The risks designated "manage" are: 1) Changing Resource Mix, 2) Cybersecurity Vulnerabilities, 3) Resource Adequacy and Performance, and 4) Critical Infrastructure Interdependencies. In addition, the report focuses on four risk profiles: 1) Grid Transformation, 2) Security Risks, 3) Extreme Events, and 4) Critical Infrastructure Interdependencies. While compliance with Reliability Standards is evaluated as part of continuous monitoring, the main focus of a mature CMEP is on how the ERO Enterprise and industry proactively identify and mitigate risks to the BPS.

The CMEP IP represents the ERO Enterprise's high-level priorities for its CMEP activities. While the ERO Enterprise will decide how to monitor 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 priorities to enhance their internal controls and compliance operations to mitigate risks to reliability and security.

Monitoring Schedules

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

- Midwest Reliability Organization (MRO)
- Northeast Power Coordinating Council, Inc. (NPCC)
- ReliabilityFirst (RF)
- SERC
- Texas RE
- Western Electricity Coordinating Council (WECC)

[1] The ERO Enterprise is 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.

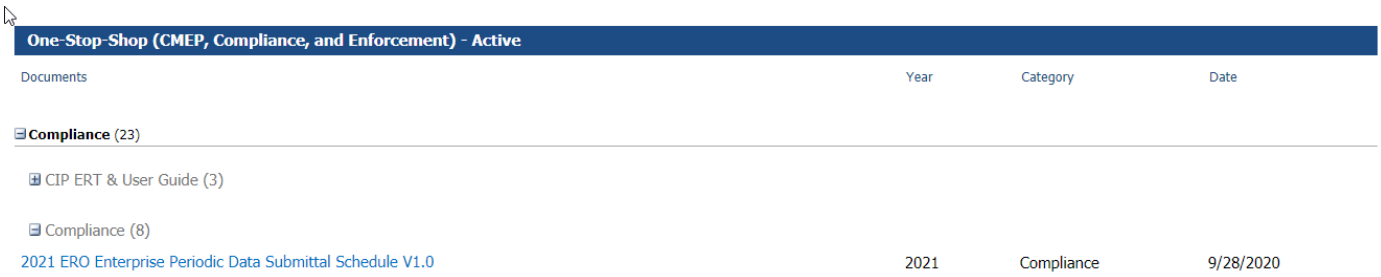
[2] NERC ROP, Appendix 4C Section 4.0 (Annual Implementation Plans).

[3] RISC ERO Priorities Report; August 2021

Periodic Data Submittals

The Compliance Enforcement Authorities (CEAs) require Periodic Data Submittals (PDS) in accordance with the schedule stated in the applicable Reliability Standards, as established by the CEA, or as needed, in accordance with the NERC ROP, Appendix 4C Section 3.6. The ERO Enterprise's data format requirements and specifications, data review processes, potential noncompliance determination processes, as well as Preliminary Screening and Enforcement actions, are managed by the ERO Enterprise. Submittal forms within Align for applicable Standard requirements are maintained by ERO Collaboration groups or are provided with the Standard.

NERC posts an annual and ERO-wide PDS schedule for awareness across Regional boundaries. The CEAs use the PDS schedule[4] posted by NERC on the NERC Compliance One-Stop Shop, located under "Compliance" at this link: NERC Compliance One-Stop Shop.



[4] In addition, WECC has two WECC Criterion on which it collects data annually (2022 WECC Periodic Data Submittal Schedule).

2022 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 the impacts from 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., the RISC). Reviewed publications include the RISC's biennial report,[6] the State of Reliability Report,[7] the Long-Term Reliability Assessment, publications from the RISC, special assessments, the ERO Enterprise Strategic Plan, ERO Event Analysis Process insights, and applicable Regional Risk Assessments. The ERO Enterprise uses these risk elements to identify and 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 2021 risk elements to determine applicability for 2022. The CMEP IP identifies NERC Reliability Standards and Requirements to be considered for focused CMEP activities. The ERO Enterprise recognizes, however, that by using the Framework and other risk-based processes, the CEAs will develop an informed list of NERC Reliability Standards and Requirements for any monitoring activities specific to a registered entity's risks. Notably, the CMEP IP is not intended to be a representation of just "important" Reliability Standard 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.

Pandemic Effects of CMEP Activities

In response to the coronavirus pandemic, in March 2020, the ERO Enterprise postponed on-site audits and other on-site activities. The ERO Enterprise continued to defer on-site activities through the end of 2021 to allow registered entities to continue to focus their resources on keeping their workforces safe and the lights on. Since March 2020, the ERO Enterprise has coordinated with registered entities on remote compliance monitoring enabled by video technology and virtual meeting platforms.

In May 2020, the ERO Enterprise released guidance[8], which provided additional regulatory relief related to registered entities' coronavirus response and temporarily expanded the Self-Logging Program. Due to the ongoing pandemic, the ERO Enterprise extended this expansion through December 31, 2021, to allow all registered entities to self-log instances of potential noncompliance with minimal or moderate risk related to their coronavirus response.

Throughout the pandemic, the ERO Enterprise recognized the importance of prioritizing the health and safety of personnel and the continued reliability and security of the BPS. We will continue to evaluate the circumstances to determine the need for additional guidance. When conditions allow, the ERO Enterprise will prioritize monitoring activities and risks that benefit the most from on-site components, including some on-site activities deferred from 2020 and 2021.

Impact of Risk Elements

The CEAs evaluate the relevance of the risk elements to the registered 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

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

[6] RISC ERO Priorities Report; August 2021

[7] NERC State of Reliability 2021

[8] ERO Enterprise Releases New Guidance Temporarily Expanding Self-Logging Program Due to Coronavirus Impacts

be more relevant to mitigate 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 2022 risk elements included in Table 2 reflect the continued maturation of the risk-based approach to compliance monitoring. The discrete risks identified within the risk elements 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.

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 understand how effectively certain obligations are being implemented and to encourage best practices to achieve the common goal of mitigating risk to the BPS. Enforcement may consider these risks when assessing risk from possible noncompliance, assisting with mitigation plans, or assessing penalties. In Q3 2021, the ERO Enterprise initiated an effort to better understand entities' implementation of CIP-008, specifically how a registered entity defines Reportable Cyber Security Incident and attempts to compromise. In Q4 2021, the ERO Enterprise will collaborate with a small number of entities to focus on the practices and controls to evaluate the effectiveness of Incident Response reporting as related to the Reliability Standard requirements (e.g., CIP-008). In addition, this year CMEP staff seeks to understand how RCs are performing their analysis and determining Interconnection Reliability Operating Limits (IROLs), including how the recommended practices outlined in the *Reliability Guideline – Methods for Establishing IROLs* have been incorporated. Aggregated information on potential industry best practices and concerns will be outlined in public reports after completion of the activities, which is expected in 2022.

The coronavirus pandemic has caused some risks to BPS Operations and the risk element descriptions have been updated slightly from 2020 to reflect some of these concerns. The risk from potential pandemics has been considered in years past as well as 2021. As identified in NERC's Preparedness and Operational Assessment, published in Spring 2020,[9] pandemic risk differs from many of the other threats facing the BPS because it is a "people event." The fundamental risk is the loss of staff critical to operating and maintaining the BPS such that firm loads could no longer be served reliably and securely. Regions may consider reviewing requirements related to personnel training in order to address this risk. In addition to short-term impacts, there are long-term impacts to consider, for example:

- Supply chain issues affecting entities' ability to acquire Bulk Electric System (BES) Assets
- Microchip supplies affecting cyber assets, specifically where entities already had aging BES Cyber Systems (BCS) or legacy systems
- Staffing shortage affected by the reduction in workforce, or, the changing landscape of the workforce as people leave jobs not allowing remote work
- Future trained staff shortage due to the slow-down in graduates and certification programs.

The 2021 risk element "Inadequate Real-time Analysis During Tool and Data Outages" was removed this year after evaluating all inputs. This risk element drove activities for CMEP staff to focus on how entities adapt to loss or degradation of Real-Time Assessment (RTA) tools and collaborating with FERC, which led to the FERC and ERO Enterprise Joint Report on Real-Time Assessment[10] released in July 2021. The 2021 RISC ERO Reliability Risk Priorities report similarly downgrades the risk from "manage" to "monitor."

[9] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Pandemic_Preparedness_and_Op_Assessment_Spring_2020.pdf

[10] https://www.ferc.gov/media/ferc-and-ero-enterprise-joint-report-real-time-assessments

Table 1: 2021 Risk Elements
Remote Connectivity and Supply Chain
Poor Quality Models Impacting Planning and Operations
Gaps in Program Execution
Determination and Prevention of Misoperations
Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages

Table 2: 2022 Risk Elements
Remote Connectivity
Supply Chain
Models Impacting Long-term and Operational Planning
Gaps in Program Execution
Protection System Coordination
Extreme Events

Remote Connectivity

The protection of critical infrastructure remains an area of significant importance. This risk element focuses on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.[11] The 2021 RISC report[12] continues to emphasize the need to control poor cyber hygiene. The 2021 State of Reliability report[13] highlights trusted third-party phishing, social engineering, and supply chain compromise as the primary cybersecurity threats to the BPS. One of the effects of the coronavirus pandemic has been changes to the designed interaction between employees, vendors, and their workspaces which could have unintended effects on the controls in place to protect critical infrastructure.

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 remote connectivity and the complexity of the tasks the individuals perform. If security has increased the difficulty in performing personnel's normal tasks, personnel may 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: 1) whether the automation was correctly configured; 2)

[11] ERO Reliability Risk Priorities; February 2018

[12] RISC ERO Priorities Report; November 2021

[13] 2021 State of Reliability report

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.[14]

Areas of Focus

Table 3: Remote Connectivity

Focused Risk	Standard	Req	Entities for	Asset Types
Remote access to Critical Infrastructure Cyber Assets introducing increased attack surface, as well as possible increased exposure.	CIP-005-6 (CIP-005-7 Effective 10/1/2022)	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
Malware detection and prevention tools deployed at multiple layers (e.g., Cyber Asset, intra-Electronic Security Perimeter and at the Electronic Access Point) are critical in maintaining a secure infrastructure.	CIP-007-6	R3	Malware detection and prevention tools deployed at multiple layers (e.g., Cyber Asset, intra-Electronic Security Perimeter and at the Electronic Access Point) are critical in maintaining a secure infrastructure.	Backup Control Centers Control Centers Data Centers Generation Facilities Substations

Supply Chain

Supply Chain risks are growing and continue to be a focal point. FERC and NERC released a Joint Staff white paper on Supply Chain vendor identification that provided noninvasive techniques that registered entities may use to identify a vendor of network interfaces deployed on their network.[15] Further, the Presidential Executive Order[16] banning specific foreign manufacturers' equipment addresses supply chain risk from international espionage that is only increasing. In addition, NERC has published several NERC Alerts on Supply Chain risks.[17] Various publications have highlighted several vendors, services, and products widely used by industry, underscoring the importance of awareness as it relates to the supply chain risks.[18] Additionally, it has been reported that security components of BES Cyber Systems may have been compromised within their respective supply chains.[19]

[14] US-CERT TA18-074A

[15] Joint Staff Whitepaper on Supply Chain

[16] Executive Order on Securing the Information and Communications Technology and Services Supply Chain

[17] NERC Alerts

[18] EPRI Supply Chain Risk Assessment Report; July 2018

[19] NATF Cyber Security Supply Chain Risk Management Guidance; June 2018

FERC and NERC E-ISAC published a NERC Alert[20] regarding the SolarWinds Orion platform and Microsoft Azure/365 Cloud compromises, highlighting large and recent supply chain attacks that had widespread implications. The SolarWinds Orion attack mainly affected key suppliers, resulting in industry being impacted downstream even though the registered entity may not have purchased, and/or installed, the infected software. Underscoring the severity of these supply chain attacks, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) required federal agencies to take action in an Emergency Directive 21-01.[21] Due to both supply chain attacks, DHS CISA developed various tools[22] to help identify compromises. Additionally, the supply chain attacks on meat processing giant JBS and Colonial Pipeline have lessons learned that can be applied to the electric sector. While these risks may create registered entity reliability issues, collectively the risks could cause BPS cascading disruptions.

Area of Focus

Table 4: Supply Chain				
Focused Risk	**Standard**	**Req**	**Entities for**	**Asset Types**
Unverified software sources and the integrity of their software may introduce malware or counterfeit software.	CIP-010-3 (CIP-010-4 Effective 10/1/2022)	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
Mitigate risks to the reliable operation of the BES by implementing sound Supply Chain policies and procedures.	CIP-013-1 (CIP-013-2 Effective 10/1/2022	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

Models Impacting Long-term and Operational Planning

Long-term and Operational Planning enable the integration and management of system assets. This includes system analyses of other emerging 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 availability of generation providing essential reliability services). NERC's annual Long-Term Reliability Assessment[23] forms the basis of NERC's assessment of emerging issues to BPS reliability. The ERO continues to raise awareness on inverter-based resource performance through NERC Alerts[24] and industry outreach. Compliance monitoring should seek to understand how entities adapt to new practices and tools to mitigate emerging risks in this continually changing environment. CMEP staff are expected to review and implement the guidance for auditing relevant requirements using the ERO Enterprise CMEP Practice Guide: Information to be Considered by CMEP Staff Regarding Inverter-Based Resources.[25]

[20] NERC SolarWinds and Related Supply Chain Alert
[21] CISA ED 21-01
[22] CISA Sparrow and Aviary
[23] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2020.pdf
[24] https://www.nerc.com/news/Documents/Inverter%20Alert%20Announcement.pdf
[25] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20Regarding%20Inverter-Based%20Resources.pdf

Inadequate long-term planning can lead to increased risks to reliability. Accurately modeled planning cases become increasingly critical as a changing resource mix, deployment of new technologies, etc., affect the risk to BPS reliability. For instance, models should reflect if power electronic controls of utility-scale inverter-based resources, such as PV resources, enable both real and reactive power generation. As stated in the NERC 2021 State of Reliability report, "The addition of variable resources, primarily wind and solar, and the retirement of conventional generation are fundamentally changing how the BPS is planned and operated. Planning and operating the grid must increasingly account for greater uncertainty across the resource fleet as well as uncertainty in electricity demand that is being affected by increasing amounts of demand-side resources."[26] The 2021 RISC report[27] states that, *"Changes in generating resources, fuel sources and fuel deliverability, energy deliverability to the load, and load characteristics are accelerating, challenging the traditional methods of long-term planning, short-term planning and real-time operations.*" 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 capacity available during peak hours.

Insufficient operational planning can lead to increased risks to reliability in the near-term. 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 industry can better understand the system is by monitoring load characteristics and the changing nature of load due to Distributed Energy Resources (DER). The 2021 ERO Reliability Risk Priorities Report states on DER, "*Distributed generation and storage (including behind the meter DERs and other DER technologies) currently follow local interconnection requirements and operational protocols that pose potential challenges to the BPS from a planning and forecasting perspective as penetration levels increase*." Further, the report states, "*The ERO Enterprise should continue its effort to address the recommendations of the Inverter-Based Resource Performance Working Group (IRPWG). Ongoing advances in inverter technologies, including those resulting from encouraging work of the IEEE P2800 equipment standard and grid-forming inverter research, should also be reflected in ongoing efforts of the IRPWG and related aspects of the ERO Enterprise. With future adoption of technical guidelines and equipment standards and soon with selective deployment of emerging grid-forming inverter technology when needed, inverter-based resources will make important contributions to BPS reliability during grid transformation.*"

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.[28]

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 understand and more accurately model inverter-based resource characteristics. NERC has identified adverse characteristics of inverter-based resources in two separate Alerts.[29,30] 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 need to be widely communicated and addressed

[26] https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2021.pdf

[27] https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf

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

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

[30] NERC Modeling Notification: Recommended Practices for Modeling Momentary Cessation Distribution; February 2018

by the industry. Entities with increasing inverter-based resources should be aware and address this within their models.[31]

Areas of Focus

Table 5: Models Impacting Long-term and Operational Planning				
Focused Risk		**Standard**	**Requirements**	**Entities for Attention**
Changing Resource Mix Resource Adequacy and Performance Critical Infrastructure Interdependencies Grid Transformation Extreme Events Loss of Situational Awareness	Ensure adequate models of generation	MOD-026-1	R2	Generator Owner Transmission Planner
		MOD-027-1	R2	Generator Owner Transmission Planner
	Ensure accurate System models for Long-term and Operational planning studies	MOD-032-1	R1, R2	Generator Owner Load Serving Entity Planning Coordinator Transmission Owner Transmission Planner
		MOD-033-1	R1, R2	Planning Coordinator Reliability Coordinator Transmission Operator
		TOP-003-4	R1	Transmission Operator Generator Owner Transmission Owner

Gaps in Program Execution

The effects of the coronavirus pandemic on the industry's ability to mitigate risk are not completely apparent. Many controls have been set up to work a certain way under specific conditions. Registered entities need to understand the effects of changes to workspace, coworker interaction, coworker availability, resource availability, contractor availability, electronic access from alternate workspaces, and other adjustments. Monitoring focus on this area can

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

help discover best practices in keeping existing controls working and effective, and in discovering what controls may need to be added.

As identified in the NERC Preparedness and Operational Assessment Spring 2020,[32] workforce availability constraints could: 1) extend the time necessary to respond to abnormal system conditions or troubleshoot and repair damaged facilities; 2) preclude necessary preventive and corrective maintenance; 3) prolong outage restoration; and 4) possibly reduce reserve margins if generating facilities are forced offline.

The coronavirus pandemic has complicated registered entity inspection and maintenance programs because of travel limitations and physical distancing requirements. Vegetation management programs need to remain a priority for registered entities to reduce the risks of vegetation contacts

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.

Monitoring and enforcement efforts seek to identify effective processes and practices by registered entities in establishing appropriate thresholds for identifying Reportable Cyber Security Incidents and defining attempts to compromise, so that they are efficiently reported to the E-ISAC in support of security and information sharing. Reliability Standard CIP-008-6 R4 provides specific requirements related to Reportable Cyber Security Incidents. The ERO Enterprise may also conduct activities in collaboration with a cross-section of registered entities to understand the effectiveness of CIP-008-6 R4 by seeking to understand how these processes are being developed and executed, whether the thresholds established are effective, and whether there are opportunities to more broadly share best practices among the industry.

[32] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Pandemic_Preparedness_and_Op_Assessment_Spring_2020.pdf

Areas of Focus

Table 5: Gaps in Program Execution				
Focused Risk	**Rationale**	**Standard**	**Requirements**	**Entities for Attention**
Change management weaknesses and Incident Reporting	Ensuring entities maintain complex programs, which handle large amounts of data (e.g., accurate inventories of equipment following asset transfers, addition of new equipment, replacement of equipment following extreme events, lack of automation, etc.)	CIP-008-6	R4	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator
		CIP-010-3	R1	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator
		FAC-003-4	R1, R2, R3, R6, R7	Generator Owner Transmission Owner
		FAC-008-5	R6	Generator Owner Transmission Owner
		PRC-005-6	R3	Generator Owner Transmission Owner

Protection System Coordination

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),[33] the August 14, 2003 Blackout (see recommendation 21),[34] and the Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015 (see recommendation 2).[35]

Of particular interest in 2022 is how entities are aware of their protection systems and how they would react during extreme events. Lack of coordination between generator protection and UFLS and/or UVLS schemes, along with local generator UF protection and behavior of inverter-based resources, can lead to unforeseen actions taken by a protection system. For example, operators performing manual load shed should avoid using circuits equipped with automatic underfrequency load shed (UFLS). If operators have already dropped those circuits, they are unavailable for further relief if the frequency drops and UFLS is needed to preserve BPS reliability.

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 or misoperations can even start cascading failures, as each successive trip can cause another

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

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

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

protection system to trip. Thorough analysis of lessons learned from misoperations can have a substantial reliability impact.

Based on early analysis, neighboring entities are seeing different short circuit fault currents at their seam locations. This is a concern from a relay coordination perspective, and the emerging standard PRC-027 seeks to address this risk. Short circuit analysis as part of the new PRC-027 Standard is needed to address this risk in a better way.

The 2021 RISC report[36] includes a descriptor of risk regarding control and protection system complexity that the ERO Enterprise, the impacted organizations, and the respective forums and trade organizations should strive to mitigate. As identified in the NERC Preparedness and Operational Assessment Spring 2020,[37] pandemic risk differs from many of the other threats facing the BPS because it is a "people event." As such, it is possible controls may be disrupted and unable to identify and correct these issues. Understanding how an entity uses controls can help promote best practices in this area.

Areas of Focus

Table 6: Protection System Coordination

Focused Risk	Rationale	Standard	Requirements	Entities for Attention
Control and Protection Systems Complexity Extreme Events	Ensure proper analysis of protection system operations.	PRC-004-6	R5	Generator Owner Transmission Owner
	Ensure UFLS schemes are designed to interact appropriately with generator protection.	PRC-006-5	R3	Planning Coordinator
	Ensure protection schemes are designed to interact appropriately with frequency and voltage excursions.	PRC-024-2 (PRC-024-3 Effective 10/1/2022)	R1, R2	Generator Owner
	Ensure proper analysis of lessons learned from misoperations.	PRC-027-1	R1, R3	Generator Owner Transmission Owner

[36] RISC ERO Priorities Report; August 2021

[37] NERC Pandemic Preparedness and Op Assessment Spring 2020

Extreme Events

Extreme events encompass a wide range of events that can cause major BPS impacts. As identified in the 2021 RISC report,[38] recent cold weather events (i.e., in ERCOT, MISO, and SPP) as well as heat events (i.e., 2020 California event) show that not only do extreme events pose challenges due to the nature and frequency of the extreme event itself, but also that the grid transformation also heightens the effects and complicates mitigation of an extreme event. Other extreme events include pandemics and threats to national security. Extreme events can stress the BPS and expose weaknesses such as poor coordination between neighboring entities in planning or operations. Extreme events can lead to a need to replace equipment, as identified in last year's CMEP IP risk element "Loss of Major Transmission Equipment with Extended Lead Times."

In light of the February 2021 Texas cold weather event, the recently expedited FERC approval[39] of the Cold Weather Reliability Standards,[40] the February 2021 Cold Weather Grid Operations: Preliminary Findings and Recommendations,[41] and the recent *Cold Weather Preparations for Extreme Weather*[42] *Events* Alert,[43] it is necessary to understand this risk. The updated Reliability Standards changed to focus on cold weather preparedness are not enforceable until April 1, 2023. Therefore, ERO Enterprise CMEP staff may find that an entity has yet to develop and implement the relevant processes and procedures. However, it is important to understand entity plans for, and progress toward, mitigating risk for the upcoming winter and going forward. CMEP staff will conduct cold weather preparedness reviews, in support of the NERC Alert, through the relevant Reliability Standards (EOP-011-2, IRO-010-4, and TOP-003-5) implementation period. The ERO Enterprise has developed a Practice Guide[44] to support understanding of this risk.

The ERO Enterprise continues to work with FERC through a joint inquiry to better understand the root causes of the cold weather outages in ERCOT, MISO, and SPP. FERC approved release of preliminary findings and recommendations[45] of the joint inquiry. Actions in the final report, when released, will be implemented and facilitated by the ERO Enterprise. Compliance monitoring and enforcement activities may be adjusted as needed to understand the efforts of industry to mitigate cold weather events in the past, considering the difference in the resource mix over time and the performance of those resources during these widespread extreme temperature events.

Weaknesses exposed in the BPS by extreme events can include:

- difficulties obtaining equipment due to pandemic
- discovery of critical infrastructure dependencies
- discovery of dependency on a resource which has diminished due to changing resource mix
- aging infrastructure coupled with less than adequate maintenance
- failure of large power transformers resulting from a Geomagnetic disturbance, wildfires, or other weather-related effect

[38] RISC ERO Priorities Report; August 2021

[39] eLibrary | File List (ferc.gov)

[40] Project 2019-06 Cold Weather (nerc.com)

[41] February 2021 Cold Weather Grid Operations: Preliminary Findings and Recommendations | Federal Energy Regulatory Commission (ferc.gov)

[42] Extreme Cold Weather as defined in the *Polar Vortex Review* dated September 2014; Extreme Cold Weather conditions occurred in lower latitudes than normal, resulting in temperatures 20 to 30° F below average.

[43] https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC%20Alert%20R-2021-08-18-01%20Extreme%20Cold%20Weather%20Events.pdf

[44] https://www.nerc.com/pa/comp/guidance/Pages/default.aspx

[45] February 2021 Cold Weather Grid Operations: Preliminary Findings and Recommendations | Federal Energy Regulatory Commission (ferc.gov)

- any type of intentional (or unintentional) physical or cyber-security breach, including the impacts of an electro-magnetic pulse (EMP)

As the BPS ages, less-than-adequate infrastructure maintenance is a reliability risk that continues to grow. The 2019 RISC report identified 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 widespread outages, and such outages could be initiated or exacerbated by equipment failures.

As the resource mix available to generate power changes, planning studies must be updated in response. If planning and resource adequacy assessments are limited in scope, extreme events can lead to unanticipated system response including widespread blackout. If operational planning does not reflect the different design and performance characteristics of new technology such as DER and inverter-based generation, registered entities may not adequately model demand during times of stress.

An entity's awareness of its Facilities that 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 2021 RISC Report: "Wildfires 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 wildfire risk is significant."[46]

Spare equipment strategy is an important aspect of restoration and recovery. The strategy and its related controls 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, Blackstart units may be retired; as a result, the 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.[47]

Recent cybersecurity events and the evolving threat landscape have highlighted a concern around the possibility of additional risks posed by possible coordinated cyberattacks. The ability to simultaneously electronically reach many BES Cyber Systems across multiple BES assets could greatly impact the reliable operations of the BPS. The ERO Enterprise has been engaged in reviews of implementation as CIP-014 risk assessments have become available. FERC-led audits, Regional Entity-led audits, and additional discussions have built a more comprehensive picture of how registered entities were looking at the language of the Standard and rolling out plans to be compliant. The ERO Enterprise found there were significant disparities with how entities were meeting the measure of the CIP-014-2 R1 requirement. While part of the CIP family of Standards, this requirement does necessitate some knowledge of how transmission-planning studies are performed to ensure that the required assessment meets the security objectives of the Standard and that it makes sense from a technical standpoint.

Although "Inadequate Real-time Analysis During Tool and Data Outages" is no longer its own risk element in 2022, it remains a focus in terms of how an entity mitigates risk during times of stress to the BPS.

[46] RISC ERO Priorities Report; August 2021

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

Areas of Focus

Table 7: Extreme Events				
Focused Risk	**Rationale**	**Standard**	**Requirements**	**Entities for Attention**
Critical Infrastructure Protection and Resiliency Extreme Events	Ensure critical substations and Control Centers are adequately protected, with sufficient incident response and recovery programs.	CIP-008-6	R1, R2	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
		CIP-009-6	R1, R2	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
		CIP-014-2	R1, R4, R5	Transmission Owner Transmission Planner
Critical Infrastructure Interdependencies Extreme Events	Ensure realistic expected generation commitment and dispatch for next-day conditions when possible.	TOP-002-4	R4	Balancing Authorities
	Ensure that unavailability of major Transmission equipment has been considered in the entity's spare equipment strategy.	TPL-001-4	R2.1.5	Planning Coordinator Transmission Planner