NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2024 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 1.0

October 2023

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 NERC and the six Regional Entities, is a highly reliable, resilient, 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 Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.

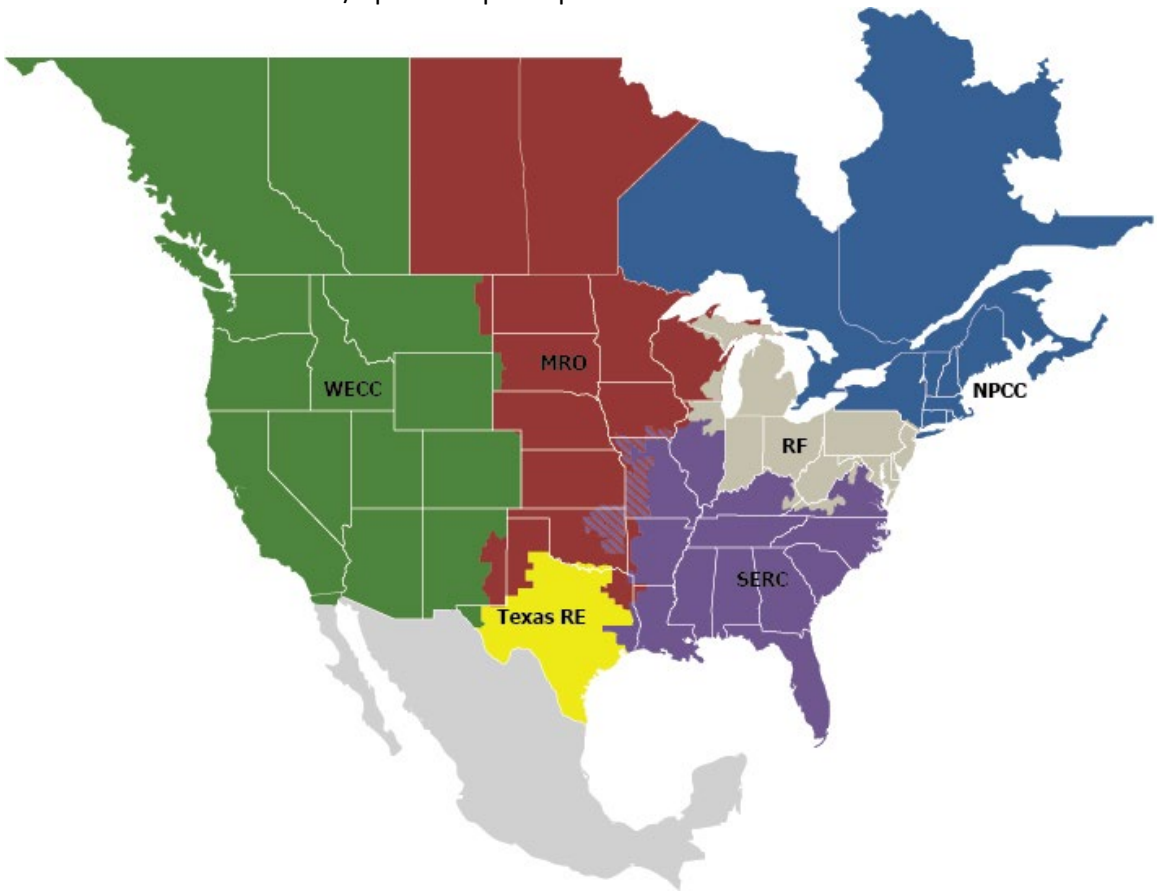

Figure 1: The Six Regional Entities of the ERO Enterprise

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 2023	• Release of the 2024 ERO CMEP Implementation Plan.

Introduction

Purpose

The Electric Reliability Organization (ERO) Enterprise[1] Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) reflects ERO and Regional Entity-specific risk elements that Compliance Enforcement Authorities (CEAs) should prioritize for oversight of registered entities. 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]

Consistent with that purpose, the 2024 ERO Enterprise CMEP IP describes the risks that will be priorities for the ERO Enterprise's CMEP activities in 2024. Collectively, NERC and each Regional Entity 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 ERO Enterprise monitoring and enforcement efforts in 2024 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 to mitigate. The risk elements described herein are all developed with the four risks designated "manage" in the 2023 RISC ERO Reliability Risk Priorities Report as well as the four risk profiles unchanged from 2021.[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 five risk profiles: 1) Grid Transformation, 2) Security Risks, 3) Extreme Events, and 4) Critical Infrastructure Interdependencies, and a new one added in 2023, 5) Policy, which will not be addressed in the 2024 CMEP IP. While compliance with Reliability Standards is evaluated as part of continuous monitoring, the 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. There is not an expectation that every risk element or every Requirement mapped to a risk element should be contained within every possible engagement. Risk elements serve as an input in determining the appropriate monitoring of risks and related Reliability Standards and requirements in the Compliance Oversight Plan (COP) for each registered entity.

[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, Section 402.1.1 and Appendix 4C Section 3.0 (Annual Implementation Plans).

[3] 2023 ERO Reliability Risk Priorities Report

Periodic Data Submittals

The 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 4.6. 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 ERO-wide PDS schedule for awareness across regional boundaries. The CEAs use the PDS schedule posted by NERC on the NERC Compliance One-Stop Shop, located under "Compliance" at this link: NERC Compliance One-Stop Shop.

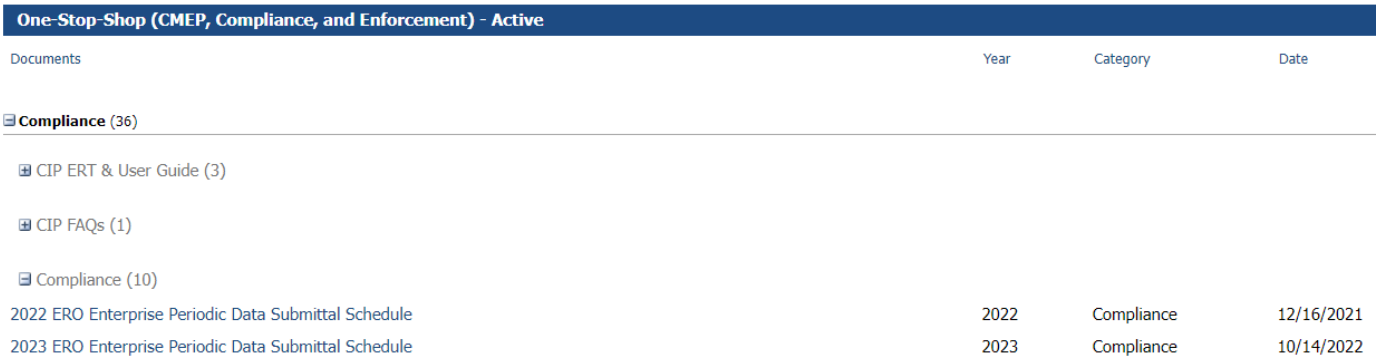

FIGURE 1: NERC One-Stop Shop

2024 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.[4] 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, [5] the State of Reliability Report, [6] 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. The ERO Enterprise uses these identified risks to focus compliance monitoring and enforcement activities.

The ERO Enterprise reviewed and reassessed the 2023 risk elements to determine applicability for 2024. 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.

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 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 2024 risk elements included in Table 1 are mostly similar to the 2023 risk elements that reflect the maturation of the risk-based approach to compliance monitoring. The changes include a new physical security risk element, and the expansion of the cold weather risk element to extreme weather, which includes both hot weather and space weather events. 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.

While some risk elements can change from year-to-year, the ERO Enterprise monitors risks from past risk elements, such as Protection System Misoperations to determine whether it is appropriate to include it as a risk element again.

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

[5] 2023 ERO Reliability Risk Priorities Report

[6] NERC State of Reliability Report 2023 Overview

Protection system misoperations remain off the list due to continued improvement with a downward trend in counts, rates, and impact metrics as identified in the 2023 State of Reliability Overview[7] report.

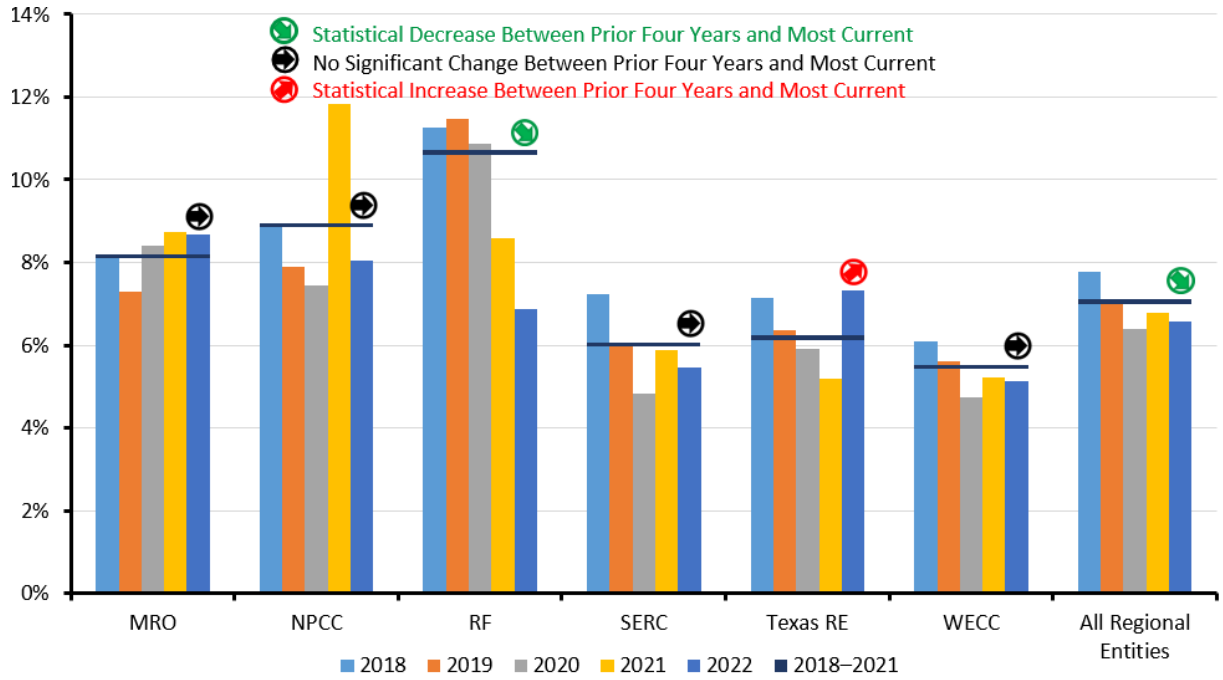

Figure 2: Changes and Trends in the Annual Misoperations Rate by Regional Entity

Table 1: 2023 and 2024 Risk Elements	
2023	**2024**
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
N/A	**Physical Security**
Incident Response	Incident Response
Stability Studies	Stability Studies
Inverter-Based Resources	Inverter-Based Resources
Facility Ratings	Facility Ratings
Cold Weather Response	**Extreme** Weather Response

[7] NERC State of Reliability Report 2023 Overview

Remote Connectivity

The protection of critical infrastructure remains an area of elevated significance. This risk element focuses on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.[8] The 2023 RISC report[9] continues to emphasize the need to control poor cyber hygiene and recommends that in order to mitigate the risk, the industry must continue to focus on early detection and response to cyber-attacks and adopt controls that can be executed to protect critical systems. The 2022 and 2023 State of Reliability report[10] highlights supply chain compromise, geopolitical events, ransomware, and physical security threats as the primary cybersecurity threats to the BPS. A lesson learned from the coronavirus pandemic across all industries has been changes to the designed interaction between employees, vendors, and their workspaces, which could have unintended effects on controls and protections of a remote workforce.

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 of personnel performing 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) controls to ensure the automation is operating as intended; and 3) access controls to manage the granting and use of access.

Harvesting credentials and exploiting physical and logical access of authorized users of Bulk Electric System (BES) facilities and BES 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.[11]

[8] ERO Reliability Risk Priorities; February 2018

[9] 2023 ERO Reliability Risk Priorities Report

[10] 2022 State of Reliability report

[11] US-CERT TA18-074A

Areas of Focus

Table 2: Remote Connectivity			
Rationale	**Standard**	**Req**	**Entities for Attention**
Remote access to Critical Infrastructure Cyber Assets introducing increased attack surface, as well as possible increased exposure.	CIP-005-7	R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
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	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
Mitigation of the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers.	CIP-012-1	R1	Balancing Authority Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

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 non-invasive techniques that registered entities may use to identify a vendor of network interfaces deployed on their network.[12] Further, the Presidential Executive Order[13] 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.[14] 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.[15] Additionally, it has been reported that security components of BES Cyber Systems may have been compromised within their respective supply chains.[16]

[12] Joint Staff Whitepaper on Supply Chain

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

[14] NERC Alerts

[15] EPRI, Supply Chain Risk Assessment Report, July 2018; Office of the Director of National Intelligence, Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains, September 2020; Microsoft, Defending the power grid against supply chain attacks, February 2020; Department of Energy, America's Strategy to Secure the Supply Chain for a Robust Clean Energy Transition, February 2022

[16] NATF, Cyber Security Supply Chain Risk Management Guidance, June 2018; Department of Homeland Security and Department of Commerce, Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry, February 2022; American Public Power Association, Shortage Changed: How Utilities Are Adapting to Supply Chain Issues, February 2022

FERC and NERC E-ISAC published a NERC Alert[17] 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 Emergency Directive 21-01.[18] Due to both supply chain attacks, DHS CISA developed various tools[19] 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. Additionally, President Biden's National Security Memorandum of July 28, 2021[20] mandated CISA to publish cross-sector cybersecurity goals and objectives for critical infrastructure control systems. The initial draft[21] covers nine common baseline controls, including supply chain.

Area of Focus

Table 3: Supply Chain			
Rationale	**Standard**	**Req**	**Entities for Attention**
Unverified software sources and the integrity of their software may introduce malware or counterfeit software.	CIP-010-4	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner
Mitigate risks to the reliable operation of the BES by implementing sound Supply Chain policies and procedures.	CIP-013-2	R1 R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

Physical Security

The number of physical security incidents continues to increase as noted in the breakdown below. Though the targets vary, many of these attacks have been carried out against substations or distribution infrastructure. In November and December, a series of high-profile attacks on substations in the Pacific Northwest and Southeast United States included vandalism, tampering, arson, and ballistic damage. While there was no impact to the BPS because of these incidents, local power disruptions did occur, impacting tens of thousands of customers.

[17] NERC, SolarWinds and Related Supply Chain Alert

[18] CISA ED 21-01

[19] CISA Sparrow and Aviary

[20] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

[21] Cross-Sector Cybersecurity Performance Goals (CPGs) Common Baseline: Controls List

Concerns regarding growing physical security threats to the BPS led FERC to issue an order that directed NERC to assess the effectiveness of Reliability Standard CIP-014-3, focusing specifically on the inclusion applicability criteria, associated risk assessments, and whether a minimum level of physical security protections should be established for all BPS transmission stations, substations, and primary control centers.[22] NERC subsequently filed a report evaluating CIP-014-3 and the risk of physical security attacks to the BPS.[23]

In addition, the potential use of drones to conduct surveillance, espionage, and physical attacks that damage electrical infrastructure also remained a concern. The E-ISAC has monitored drone activity data gathered in late 2022 and is currently conducting a 12-month pilot to provide asset owners and operators with a baseline understanding of the level of drone activity around electric infrastructure. Analysis related to this effort will be shared through the E-ISAC Portal in 2023.[24] Some of the largest risks are considered to be co-dependence with cyber security (e.g., computer controls for physical access) and the prospective impact of replacing long lead-time equipment (e.g., large power transformers) damaged during an attack.[25]

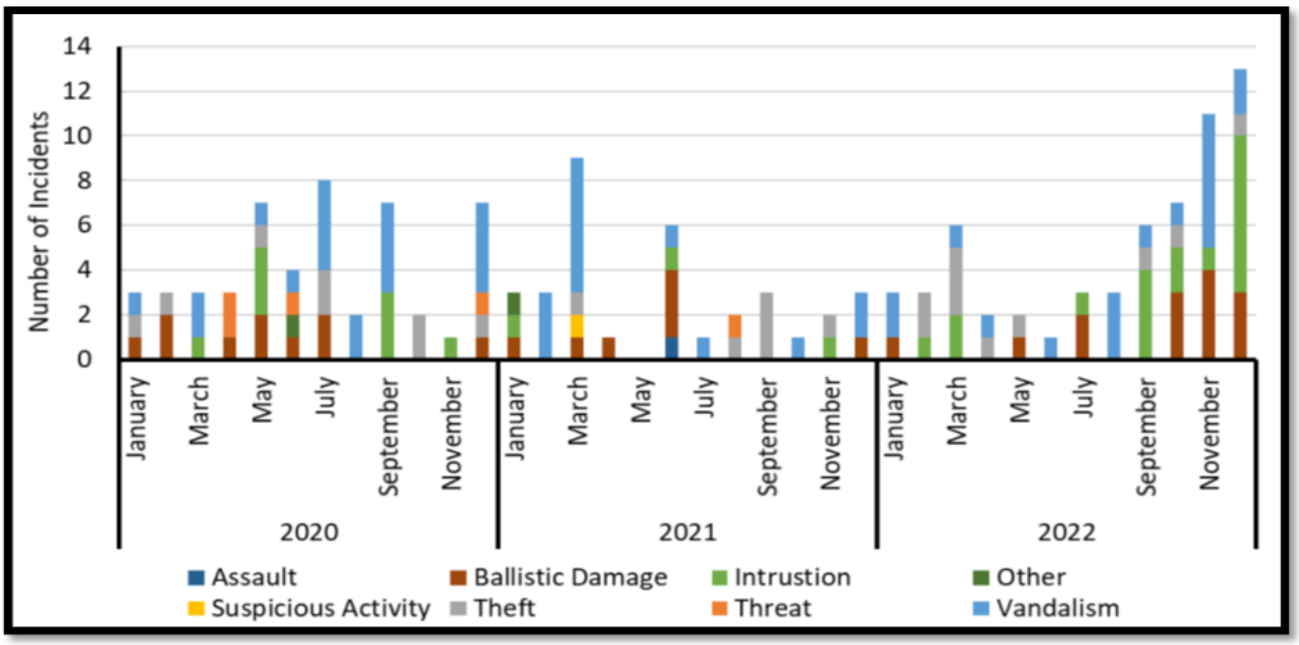

Figure 3: Level 2 and Level 3 Breakdown of Incident Types for 2020–2022

[22] 2023 State of Reliability Technical Assessment

[23] NERC Report on CIP-014-3

[24] 2023 State of Reliability Technical Assessment

[25] 2023 ERO Reliability Risk Priorities Report

Area of Focus

Table 4: Physical Security[26]			
Rationale	**Standard**	**Req**	**Entities for Attention**
Mitigate risks to the reliable operation of the BES as the result of a Physical Security Incident.	CIP-014-3	R4, R5	Transmission Operator Transmission Owner

Incident Response

Incident response has increasingly emerged as a risk to the BPS. Dragos has published a white paper[27] on the malware developed by threat group Chernovite named Pipedream. This malware targets industrial control systems, including the electric sector. One of the long-term readiness best practices within this white paper is to have an updated industrial control system-focused incident response plan with accompanying Standard Operating Procedures and Emergency Operating Procedures for operating with a hampered or degraded control system. Additionally, the CISA Cross-Sector CPGs Common Baseline includes the need to develop, maintain, and practice incident response plans to ensure effective response to threat actions against all assets, along with reporting cybersecurity incidents across IT and OT assets to CISA and any other mandatory reporting stakeholders. Another tool that could be beneficial is the continuation of efforts like the Cybersecurity Risk Information Sharing Program or other programs similar in nature.[28] There are many additional efforts underway to develop cyber tools and frameworks that should assist industry in enhancing preparation and reaction plans according to the 2023 ERO Reliability Risk Priorities Report.

Area of Focus

Table 5: Incident Response			
Rationale	**Standard**	**Req**	**Entities for Attention**
Mitigate risks to the reliable operation of the BES as the result of a Cyber Security Incident.	CIP-008-6	R1, R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

Stability Studies

The ERO Enterprise continues to make steady progress in evaluating operational and transmission planning impacts resulting from the changing resource mix. The NERC 2022 Long-term Reliability Assessment highlights BPS risks associated with inverter-based resources (IBRs).[29] In particular, events with tripping of IBRs during disturbances are increasing in both frequency and severity. Unexpected tripping of IBRs indicates issues with dynamic model accuracy as well as issues with the robustness and thoroughness of stability studies. The ERO Enterprise has released new guidance documents pertaining to modeling verification practices that should be incorporated to sufficiently address

[26] https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20Report%20on%20CIP-014-3.pdf

[27] Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems

[28] 2023 ERO Reliability Risk Priorities Report

[29] NERC Long-term Reliability Assessment 2022

grid transformation impacts.[30] Industry adaptation to recent guidance will also require incremental improvements in stability studies performed for both long-term and operational planning to provide assurance adverse system conditions are being effectively identified and corrected.

Also, the NERC 2022 Odessa Disturbance report[31] points to insufficient model quality checks throughout the interconnection study process to avoid discrepancies between modeled and actual performance. In particular, current plant commissioning practices appear to have significant shortfalls for ensuring plant configuration matches TP, PC, and TO expectations (based on studies).

CMEP reviews of transmission planning studies have traditionally focused more heavily on the development of Contingency lists as well as steady-state studies. Building off that knowledge, CMEP staff may further seek to understand how entities are effectively studying within the time-domain to preemptively identify system performance issues following simulated system disturbances. The selection of cases, Contingencies, and monitored elements should be evaluated for robustness. The selection of criteria and thresholds should be evaluated for appropriateness, thoroughness, and alignment between neighboring entities. This risk may also be associated with incorrect protection system settings and modeling inaccuracies. These other areas should be considered as additional areas to investigate to gain assurance stability studies are effective.

Areas of Focus

Table 6: Stability Studies			
Rationale	**Standard**	**Req**	**Entities for Attention**
Planning studies are effective in identifying system performance issues following both minor and major system disturbances.	CIP-014-3	R1	Transmission Owner
	TPL-001-4, TPL-001-5.1	R4, R6	Planning Coordinator Transmission Planner

Inverter-Based Resources

Analyses of system events have shown a need to understand and more accurately model IBR characteristics. NERC has identified adverse characteristics of IBRs in two separate Alerts.[32,33] NERC has also released detailed reports about disturbances within 2021-2023, three in Texas[34],[35] two in California,[36], and one in Utah[37], which strongly recommend that industry take timely action to implement all of the recommendations set forth within the disturbance reports and related NERC reliability guidelines. 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 by the industry. Entities with increasing IBRs should be aware and address

[30] RTSC Approved Reliability Guidelines (see under EGWG and IRPS)

[31] NERC 2022 Odessa Disturbance Report

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

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

[34] Odessa Disturbance Texas Events: May 9, 2021 and June 26, 2021 Joint NERC and Texas RE Staff Report; September 2021

[35] 2022 Odessa Disturbance: June 4, 2022 Joint NERC and Texas RE Staff Report; December 2022

[36] Multiple Solar PV Disturbances in CAISO Disturbances between June and August 2021; April 2022

[37] Southwest UT Solar PV Disturbance 2023

this within their models.[38] In 2023, the focus remains as the 2023 State of Reliability Technical Assessment[39] finds that, in order for the BES to continue benefiting from the rapid expansion of inverter-based resources, their dynamic performance during system events must improve. It goes on to say that the risk profile for IBR performance issues needs to be elevated, and immediate ERO Enterprise risk-based compliance activities are needed in this area. Also of interest is the RSTC Reliability Guideline from March 2023[40] which provides recommendations for TPs, PCs, GOs, equipment manufacturers, and consultants conducting EMT modeling and studies for inverter-based resources. NERC strongly encourages these entities to adopt all of the recommendations contained throughout that guideline.

The Texas[41] and California[42] reports identify that solar PV plants lack sufficient ride-through capability to support the BPS for normal BPS fault events. This reliability concern is persistent, growing in the number of resources prone to this issue, not being mitigated appropriately, and warrants mitigating actions.

CMEP staff are expected to review and consider the guidance for auditing relevant requirements using the *ERO Enterprise CMEP Practice Guide: Information to be Considered by CMEP Staff Regarding Inverter-Based Resources*.[43]

For transparency, NERC's Inverter-Based Resource Strategy was released in September 2022.[44]

Area of Focus

Table 7: Inverter-Based Resources			
Rationale	**Standard**	**Req**	**Entities for Attention**
Clear and consistent interconnection requirements for IBRs	FAC-001-4	R1, R2	Generator Owner Transmission Owner
IBRs being adequately studied during the interconnection process	FAC-002-4	R1, R2	Generator Owner Planning Coordinator Transmission Planner
IBRs including in models provided from generator owners	MOD-026-1	R2	Generator Owner
IBRs staying online when needed	PRC-024-3	R1, R2	Generator Owner

Facility Ratings

The accuracy of Facility Ratings is a cornerstone of being able to use and protect the BES. Inaccurate Facility Ratings undermine the usefulness of Stability Studies, which is another risk element identified earlier in this CMEP IP. Operators depend on Facility Ratings to provide reliable System Operating Limits (SOLs) and Interconnection Reliability

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

[39] 2023 State of Reliability Technical Assessment

[40] Reliability Guideline: Electromagnetic Transient Modeling for BPS Connected Inverter-Based Resources

[41] Odessa Disturbance Texas Events: May 9, 2021 and June 26, 2021 Joint NERC and Texas RE Staff Report; September 2021

[42] Multiple Solar PV Disturbances in CAISO Disturbances between June and August 2021; April 2022

[43] ERO Enterprise CMEP Practice Guide Regarding Inverter-Based Resources

[44] NERC IBR Strategy

Operating Limits (IROLs) that inform operating decisions. Protection engineers rely on Facility Ratings to protect equipment from damage while also allowing equipment to stay online when it is both safe and most needed. Some registered entities have Facility Ratings based on inaccurate equipment inventories, or ratings are not being updated during projects or following severe weather.

Given its importance, CMEP staff are urged to understand the controls that it has put in place to track Facility Ratings, which can be a large amount of data. Knowing how an entity has established an accurate baseline for its data, and how it handles any changes going forward from that baseline, can give a good indication of if an entity is struggling. NERC has released a publicly available Practice Guide to assist ERO Enterprise staff in performing their duties.[45] CMEP staff is monitoring the progress of the NERC Facility Ratings Task Force (FRTF)[46], which is currently working to address risks and technical analysis associated with the FAC-008, Facility Ratings Standards. The potential areas this task force is evaluating relate to alignment of industry's processes and procedures to assess risk and analytics and prioritize resources with those processes and procedures that focus on prioritization of reliability risks and corresponding resources.

FERC Order 881[47] will lead to changes by mid-2025 in how some entities define and use Facility Ratings, which will increase accuracy of transmission system capabilities based on actual conditions. ERO Enterprise activities will continue to focus on accurate transmission ratings, as the equipment identification risk is not changing. Once FERC Order 881 comes into effect, ERO Enterprise staff will focus on a successful implementation for Transmission Owners who have to update their methodology to clearly document ambient rating calculation methods.

The ERO Enterprise Themes and Best Practices for Sustaining Accurate Facility Ratings report[48] contains a myriad of references concerning Facility Ratings from multiple sources in the ERO Enterprise as well as the NATF. It also contains best practices to help deal with four themes: 1) Lack of Awareness, 2) Inadequate Asset and Data Management, 3) Inadequate Change Management, and 4) Inconsistent Development and Application of Facility Ratings Methodology.

Area of Focus

Table 8: Facility Ratings			
Rationale	**Standard**	**Req**	**Entities for Attention**
Ensuring entities maintain accurate Facility Ratings	FAC-008-5	R6	Generator Owner Transmission Owner

Extreme Weather Response

Extreme weather events encompass a wide range of situations that can cause major BPS impacts. As identified in the 2023 RISC report,[49] not only do recent cold weather events pose challenges due to the nature and frequency of the events themselves, but also that grid transformation heightens the effects and complicates mitigation of the event. Cold weather events can stress the BPS and expose weaknesses such as poor coordination between neighboring entities in planning or operations. Extreme heat events have also had significant impacts on the BPS. All aspects of power generation and transmission are affected by high temperatures. Higher temperatures can squeeze electricity supplies by reducing the efficiency and capacity of traditional thermal power plants, such as coal, natural gas and

[45] ERO Enterprise CMEP Practice Guide Evaluation of Facility Ratings and System Operating Limits

[46] Facility Ratings Task Force (FRTF) (nerc.com)

[47] FERC Order 881 does not apply to Texas RE. *Managing Transmission Line Ratings*, 177 FERC ¶ 61,179 (2021).

[48] ERO Enterprise Themes and Best Practices for Sustaining Accurate Facility Ratings

[49] 2023 ERO Reliability Risk Priorities Report

nuclear.[50] Additionally, transmission lines can lose efficiency due to higher resistive losses at elevated temperatures. Geomagnetic disturbance events (GMD) are also a rising concern as the BPS footprint expands. It has been noted that GMDs can impact the utility industry, especially the transmission system. The NOAA Space Weather Prediction Center recently upgraded the model it uses to improve nowcasts of regional space weather impact information for electric power operators.[51]

As revealed in the 2023 RISC report, the 2022 Emerging Risks Survey shows respondents to rank risks based on their perception, and Extreme Events came in fourth behind Changing Resource Mix, Resource Adequacy and Performance, and Cybersecurity Vulnerabilities. Although Extreme Events was the fourth item ranked as a critical risk by industry, this contrasts with the most recent State of Reliability report[52] that noted Extreme Events pose the greatest risk to reliability and stability. In 2022, the National Oceanic and Atmospheric Administration (NOAA) identified 18 separate billion-dollar weather-related disasters in the United States as noted below in Figure 4.[53]

This risk element needs to be understood in light of: the recently expedited FERC approval[54] of the Cold Weather Reliability Standards,[55] the November 2021 release of the FERC - NERC - Regional Entity Staff Report: The February 2021 Cold Weather Outages in Texas and the South Central United States,[56] and the *Cold Weather Preparations for Extreme Weather*[57] *Events* Alert.[58] The updated Reliability Standards changed to focus on cold weather preparedness were enforceable in the United States on April 1, 2023. Therefore, ERO Enterprise CMEP staff should find that an entity has developed and implemented the relevant processes and procedures. It is important to understand entity plans for, and progress toward, mitigating risk for the upcoming winter and going forward. During 2021-2023, NERC Alerts has issued recommendations and essential actions through a three-part series of Cold Weather Preparations for Extreme Weather Events[59,60,61] alerts along with an Industry Advisory alert[62]. Also, the RTSC has updated an associated Reliability Guideline[63] concerning generating unit weather readiness, expanding it for generator types. In 2023, the ERO Enterprise offered Cold Weather Preparedness Small Group Advisory Sessions (SGAS) to provide an educational opportunity for registered entities to meet with NERC and Regional Entity representatives to discuss the cold weather preparedness Standards and possible compliance approaches in an open and non-audit environment. During the course of those discussions, the NERC and Regional Entity representatives provided guidance on specific approaches for implementing Reliability Standards EOP-011-2, IRO-010-4, and TOP-003-5. The slides from the general session are available. [64]

[50] The world's electricity systems must be ready to counter the growing climate threat – Analysis - IEA

[51] NOAA upgrades space weather model used by the electric power industry

[52] 2023 State of Reliability Technical Assessment

[53] 2023 State of Reliability Technical Assessment

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

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

[56] FERC - NERC - Regional Entity Staff Report: The February 2021 Cold Weather Outages in Texas and the South Central United States

[57] 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.

[58] NERC Alert R-2021-08-18-01 Extreme Cold Weather Events

[59] NERC Alert R-2021-08-18-01 Extreme Cold Weather Events

[60] NERC Alert R-2022-09-12-01 Cold Weather Events

[61] NERC Level 3 Alert Essential Actions to Industry Cold Weather Preparations for Extreme Weather Events III

[62] NERC Alert A-2023-02-13-01 Cold Weather 2023

[63] Reliability Guideline: Generating Unit Winter Weather Readiness - Version 4 (nerc.com)

[64] Cold Weather Preparedness Small Group Advisory Sessions - General Session.pdf (nerc.com)

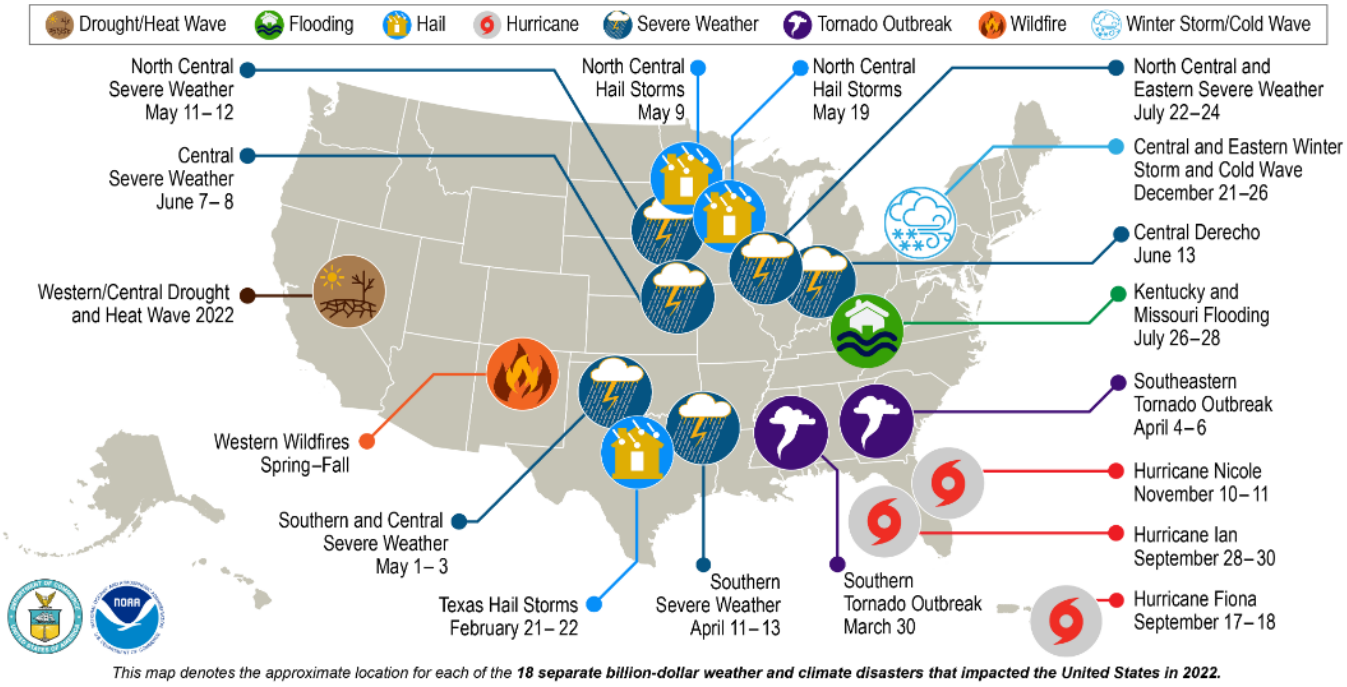

Figure 4: 2022 U.S. Billion-Dollar Weather and Climate Disasters

Areas of Focus

Table 9: Extreme Weather Response			
Rationale	**Standard**	**Req**	**Entities for Attention**
Ensure plans are developed and implemented to mitigate operating Emergencies	EOP-011-2	R1, R2, R3, R6, R7, R8	Balancing Authority Generator Owner Reliability Coordinator Transmission Operator
Ensure plans are developed and implemented to mitigate extreme cold weather	EOP-012-1 (comes into effect October 2024)	R1, R2, R3, R4, R5, R6, R7	Generator Owner Generator Operator
Planned performance during geomagnetic disturbance (GMD) events.	TPL-007-4	R1, R2, R4, R5, R7	Planning Coordinator Transmission Planner