NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2025 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

October 2024

RELIABILITY | RESILIENCE | SECURITY




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

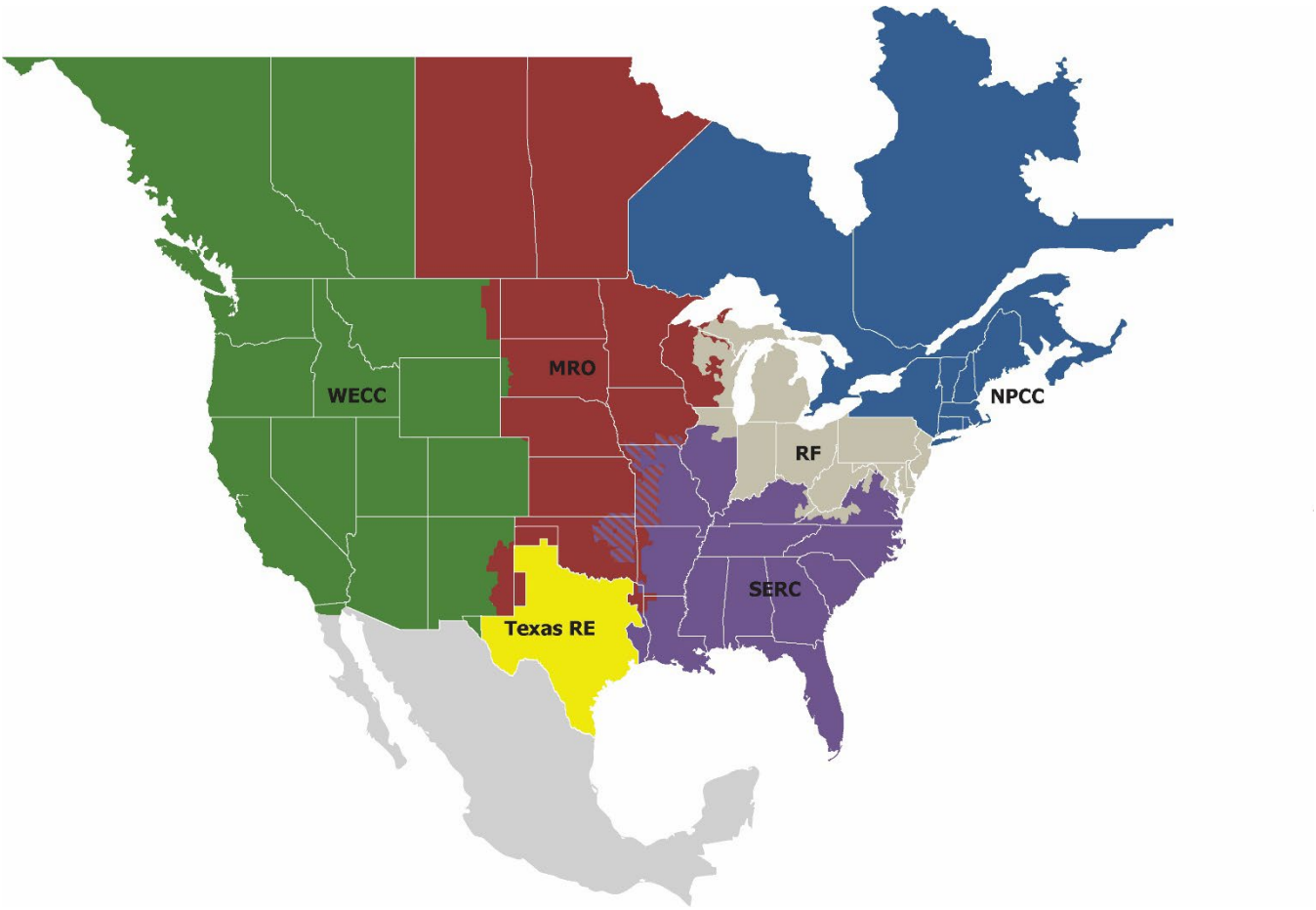
Table of Contents

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 Entities as shown on the map and in the 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.



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

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]

The ERO Enterprise is pleased to release the 2025 CMEP IP describing the risks that will be priorities for the ERO Enterprise's CMEP activities in 2025. Collectively, NERC and each Regional Entity have worked collaboratively throughout this CMEP IP's development to evaluate reports of NERC committees, 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 2025 on the risk elements identified within. The CMEP IP gives guidance to ERO Enterprise staff involved with monitoring and enforcement and, through public posting, informs the ongoing conversations with industry stakeholders about risks to the BPS. 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 for each registered entity.

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 Reliability Standard requirements are maintained by ERO Collaboration groups or are provided with the Reliability 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.

[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 3.0 (Annual Implementation Plans).

One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active

Documents	Year	Category	Date
Compliance (40)			
CIP ERT & User Guide (3)			
Compliance (13)			
2023 ERO Enterprise Periodic Data Submittal Schedule	2023	Compliance	10/14/2022
2024 ERO Enterprise Periodic Data Submittal Schedule	2024	Compliance	5/2/2024
2025 ERO Enterprise Periodic Data Submittal Schedule	2024	Compliance	11/5/2024

2025 ERO Enterprise Risk Elements

Process for Risk Elements and Associated Areas of Focus

The ERO Enterprise uses the ERO Enterprise Risk-based Compliance Monitoring approach 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.[3] 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 Reliability Issues Steering Committee RISC). Reviewed publications include the 2024 State of Reliability Report[4], 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 2024 risk elements to determine applicability for 2025. 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.

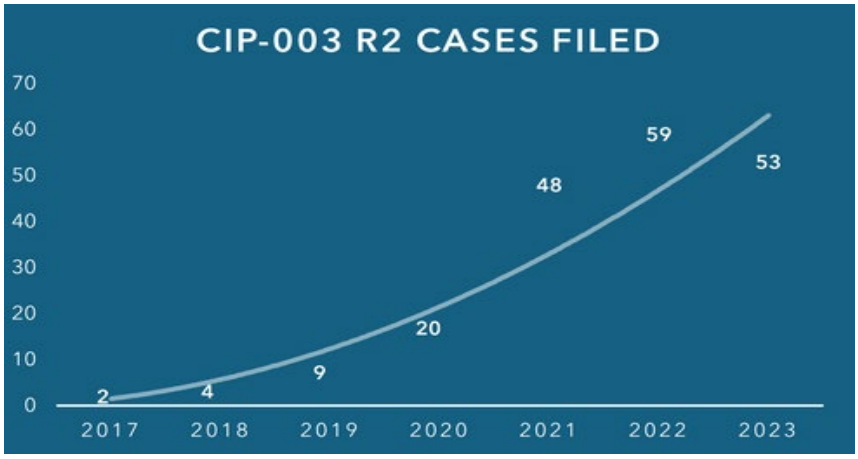
The 2025 risk elements included in Table 1 are similar to the 2024 risk elements that reflect the maturation of the risk-based approach to compliance monitoring. The changes include a new transmission and planning risk element which includes the associated risks seen in 2024 stability study risk area, and the expansion of the Inverter-based resource risk element focus on system protection measures as these assets continue to come online with increased numbers. 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.

[3] Appendix C, ERO Enterprise Guide for Compliance Monitoring; October 2016
[4] NERC State of Reliability Report 2024 Overview

Table 1: 2024 and 2025 Risk Elements	
2024	**2025**
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
Physical Security	Physical Security
Incident Response	Incident Response
Stability Studies	**Transmission Planning and Modeling**
Inverter-Based Resources	Inverter-Based Resources
Facility Ratings	Facility Ratings
Extreme Weather Response	Extreme Weather Response

Remote Connectivity



The protection of critical infrastructure remains a major focus for the 2025 risk areas. With remote connectivity and the use of remote workers continuing, it is vitally important that facility staff understand the changes taking place with their technology and have a better understanding of how to protect it. The ERO Enterprise has seen poor security practices (a) remotely unlocking doors for unauthorized individuals; (b) neglecting to secure doors and manage keys; and (c) generally failing to identify a need to create or apply security plans to new sites or sites transitioning from medium/high to low impact.[5] Root causes in these cases often point to ineffective training and lack of direction or guidance, which can result in staff treating low impact sites as functionally out of scope for NERC CIP purposes, which in turn can increase the frequency of less-than-desirable security decisions.

As security needs evolve, the ERO Enterprise and industry must remain vigilant, identify any gaps, and mitigate, as necessary. There is a noticeable trend as it relates to low impact BES Cyber Systems. As noted in the 2024 CIP Themes and Lessons Learned Report, a compromise of such assets could create localized issues, and an individual low impact asset could (a) serve as a channel to attack other assets or (b) be used to conduct reconnaissance. And the potential risk to the BES multiplies in scenarios where several low impact assets are compromised in a coordinated attack.[6]

Regardless of the sophistication of a security system across all types of BES facilities, 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.

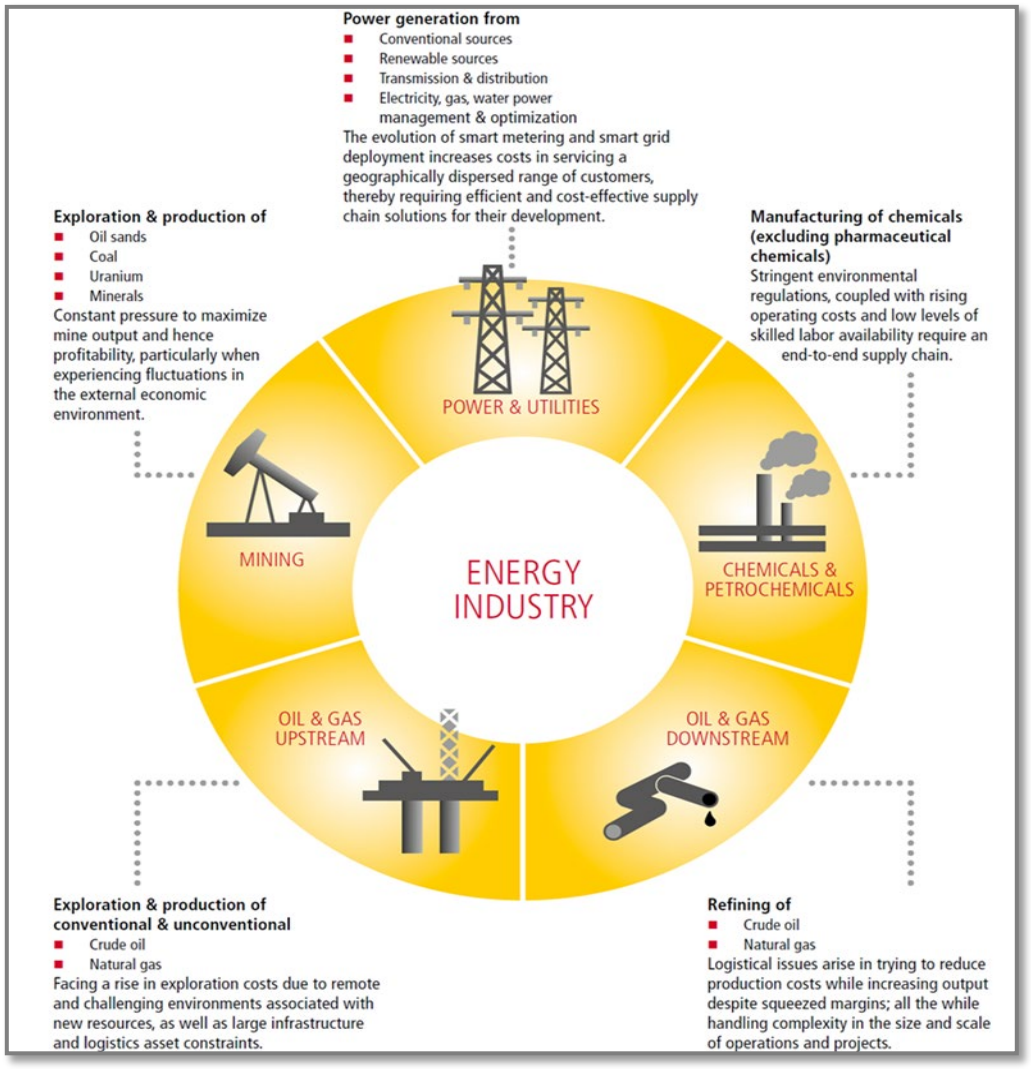
[5] 2024 CIP Themes and Lessons Learned (rfirst.org)
[6] 2024 CIP Themes and Lessons Learned (rfirst.org)

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
Reviewing more crucial procedures concerning remote access and a focus on the implementation of low impact programs.	CIP-003-8	R2	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 continue to be a focal point in various areas for the industry. Lead times for transformers, circuit breakers, transmission cables, switchgears, and insulators have increased significantly since 2020. Additionally, photovoltaic (PV) panels are more difficult to procure. These issues are delaying multiple projects in many areas such as new resource and transmission projects.[7] Further, supply chain bottlenecks have also been a major headache for developers. A lack of supply chain capacity has caused issues with high-voltage electrical equipment, skilled grid connection construction firms, wind installation vessels, data chips, and critical minerals. As a consequence, many developers are at risk of not receiving critical deliveries on time,[8] underscoring the importance of awareness as it relates to the supply chain risks.



The energy market today is both maturing and unstable, characterized by rising demand and fluctuating supply.[9] According to the International Energy Agency (IEA), global energy demand will grow by one-third between 2010 and 2035.[10] Most of this increase will come from emerging markets. But the bigger challenges arise from demand planning and forecast accuracy and with that, the alignment of materials and supply with energy usage.[11] Supply chains for oil and gas equipment and services are relatively fragmented and geographically diverse, with suppliers from Europe, the U.S., Russia, the Middle East, and mainland China. However, the renewable energy supply chain is heavily concentrated, dominated by a few suppliers and with a clear concentration in China and a handful of other nations for mineral extraction. This makes renewables more vulnerable to sourcing risks than oil and gas, as there are fewer supplier options and a greater reliance on specific countries or regions. This means procurement officers within renewables have a greater need to apply careful risk management.[12]

[7] 2024 Summer Reliability Assessment (nerc.com)
[8] Energy sector risks puts spotlight on procurement strategies | WorkBoat
[9] The Power Behind The Energy Supply Chain
[10] The Power Behind The Energy Supply Chain
[11] The Power Behind The Energy Supply Chain
[12] Workboat - Energy Strategies

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

Physical security threats continue to be a top concern in 2025 as threat levels have remained elevated. An area of particular focus should be opportunistic domestic violent extremists. They aim to exploit potential social unrest such as political elections, economic issues, and activistic causes to target infrastructure.[13] More than ever, there are more entities with assets that contain low impact BES Cyber Systems being registered across the ERO. There needs to be a concerted effort around these assets that contain low impact BES Cyber Systems as there has been an upward trend in violations regarding physical security plans, electronic security perimeters, and access management and revocation to name a few.[14] One of the many challenges of executing a physical security program is managing tasks that require repetitive behavior over significant periods of time, as there is increased potential for personnel to lose focus on the performance of an individual act or forget the importance of the act itself. Examples of this behavior that has been observed would be that in multiple instances, an employee who was running late to a shift, without their badge, was able to talk their way through multiple barriers and into a Physical Security Perimeter (PSP).[15] This theme highlights examples of apathy, circumvention, complacency, inattentiveness, and other types of "performance drift" in physical security programs at entities of every size and type.[16]

[13] 2023 E-ISAC End-of-Year Report.pdf (nerc.com)
[14] 2024 CIP Themes and Lessons Learned (rfirst.org)
[15] 2024 CIP Themes and Lessons Learned (rfirst.org)
[16] 2024 CIP Themes and Lessons Learned (rfirst.org)

Area of Focus

Table 4: Physical Security			
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
Mitigate risks to the reliable operation of the BES as the result of increased Physical Security events related to low impact assets.	CIP-003-8	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

Incident Response

Incident response continues to be a significant risk to the BPS. As attacks such as ransomware increase, industry stakeholders must continue to test and mature our response coordination capabilities throughout the ERO. "Our goal is for the National Cyber Incident Response Plan to provide an agile, actionable framework that can be actively used by every organization involved in cyber incident response to ensure coherent coordination that matches the pace of our adversaries," said Eric Goldstein, Executive Assistant Director for Cybersecurity. "The success of this effort depends on the involvement of our partners – our output will only be as good as our input. Through our shared efforts, we will build a new NCRIP that helps our nation, and our allies more effectively respond to and recover from cyber incidents in a manner that reduces harm to every possible victim."[17]

Through the Joint Cyber Defense Collaborative (JCDC), CISA will work to ensure that the updated NCIRP addresses significant changes in policy and cyber operations since the initial NCIRP was released, including:

- Establishment of CISA and ONCD;
- Maturation of private sector incident response and coordination capabilities;
- Increased international collaboration around cyber incident response and coordination;
- Shifts in the threat environment, including the ongoing ransomware threats and advances in adversary capabilities; and
- New authorities, policies, and coordination mechanisms.[18]

[17] CISA Announces Effort to Revise the National Cyber Incident Response Plan | CISA
[18] CISA Announces Effort to Revise the National Cyber Incident Response Plan | CISA

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
Ensuring continuous improvement of incident response plans after a rise in low impact events.	CIP-003-8	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner

Transmission Planning and Modeling

Over the last several years, the ERO Enterprise has released multiple detailed disturbance reports related to inverter-based resource (IBR) performance. The reports identified that IBR facilities have technical capabilities that require a deeper understanding. The lack of sufficient ride-through capability to support the BPS for fault events was a significant finding in several reports. In addition, the reports also discussed that system planning assessments need to accurately capture these types of systemic performance issues.

Planners (Planning Coordinators and Transmission Planners) are continuing to modify processes and tools to better model the contribution of IBRs to recognize the impact to reliable operations. Because of the continuing increased penetration of IBRs, the ERO Enterprise is enhancing reliability assessments to incorporate probabilistic energy assessment analyses into performance assessment products. Further, flexible resources such as batteries and demand response capabilities are being incorporated into the industry's planning processes to more accurately reflect the needed balance of demand and load. Other factors, such as large loads, data centers, and population growth are being incorporated as load growth continues to increase.

Recent issuances from the Federal Energy Regulatory Commission (FERC) also focus on modeling inverter-based resources. FERC Order 901 directed NERC to develop new or modified Reliability Standards including ones that address reliability gaps related to IBRs in model validation and planning. FERC Order 2023 requires interconnection customers requesting to interconnect an asynchronous generating facility to provide the Transmission Provider with the models needed for accurate interconnection studies.[19]

In 2023 the Reliability and Security Technical Committee released two Reliability Guidelines: *EMT for BPS-Connected Inverter-Based Resources—Recommended Model Requirements and Verification Practices* and *Performance, Modeling, and Simulations of BPS-Connected Battery Energy Storage Systems and Hybrid Power Plants*. The ERO Enterprise encourages registered entities to implement the recommendations contained within each Reliability Guideline to support reliable operations.

[19] https://www.ferc.gov/media/order-no-2023

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*.

Areas of Focus

Table 6: Transmission Planning and Modeling			
Rationale	**Standard**	**Req**	**Entities for Attention**
Address load growth concerns. Ensure proper transmission planning and modeling and proper use of data mining and modeling data.	CIP-014-3	R1	Transmission Owner
	TPL-001-5.1	R1, R2, R3, R4, R5, R6, R7	Planning Coordinator Transmission Planner
	MOD-025-2	R1, R2, R3	Generator Owner Transmission Owner
	MOD-026-1	R6	Transmission Planner
	MOD-027-1	R5	Transmission Planner
	MOD-031-3	R1, R2	Planning Coordinator Transmission Planner Balancing Authority Resource Planner Distribution Provider
	MOD-032-1	R1, R2, R3, R4	Balancing Authority Generator Owner Planning Coordinator Transmission Owner Transmission Planner Transmission Service Provider

Inverter-Based Resources

A focus remains on Inverter-Based Resources (IBR) as these assets continue to become a major part of the BPS. IBRs include most solar and wind generation as well as new battery energy storage systems (BESS) or hybrid generation and account for over 70% of the new generation in development for connecting to the BPS. IBRs respond to disturbances and dynamic conditions based on programmed logic and inverter controls.[20] As protection schemes continue to be developed, unexpected tripping of IBRs during grid disturbances continues to spread, underscoring the need for operator vigilance in the near term and urgent industry action on long-term solutions.[21] A common thread with these tripping events is the lack of IBR ride-through capability that causes a minor system disturbance to become a major disturbance. In March 2023, NERC issued the Inverter-Based Resource Performance Issues Alert to Generator Owners (GO) of Bulk Electric System (BES) solar PV generating resources.[22] As a Level 2 alert, it contains recommended actions for GOs of grid-connected solar PV resources, including steps to coordinate protection and controller settings, so that the resources will remain reliable during grid disturbances.[23]

[20] 2023 Long-Term Reliability Assessment(nerc.com)
[21] 2024 Summer Reliability Assessment (nerc.com)
[22] 2024 Summer Reliability Assessment (nerc.com)
[23] 2024 Summer Reliability Assessment (nerc.com)

In addition to a focus on system protection, a continued intentional approach is required to study the effects of IBRs on the BPS. Increases in new types of generation resources, storage, inverter-based resources connected at lower voltages (including consumer owned), and other resources that could include vehicle-to-grid delivery—have complicated the use of traditional criteria, metrics, methods, and tools for calculating resource adequacy. Moreover, the newness of the technologies has made it difficult to gather enough operational data to characterize their probabilistic behavior needed for such calculations (e.g., correlation between generation from various renewable resources and load).[24]

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	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
Document and implement programs for the maintenance of all Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying affecting the reliability of the bulk power system (BPS) so that they are kept in working order.	PRC-005-6	R3, R5	Distribution Provider Generator Owner Transmission Owner
IBRs staying online when needed	PRC-024-3	R1, R2	Generator Owner
Coordination of Protection Systems installed to detect and isolate Faults on Bulk Electric System (BES) Elements, such that those Protection Systems operate in the intended sequence during Faults	PRC-027-1	R1, R2, R3	Transmission Owner Generator Owner Distribution Provider

[24] Evolving Planning Criteria for a Sustainable Power Grid: A Workshop Report, June 2024 (nerc.com)

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 transmission planning and modeling, 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 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 an entity's 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 CMEP Practice Guide to assist ERO Enterprise staff in performing their duties.[25] CMEP staff is monitoring the progress of the NERC Facility Ratings Task Force (FRTF)[26], 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[27] 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 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[28] 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

[25] ERO Enterprise CMEP Practice Guide Evaluation of Facility Ratings and System Operating Limits
[26] Facility Ratings Task Force (FRTF) (nerc.com)
[27] FERC Order 881 does not apply to Texas RE
[28] ERO Enterprise Themes and Best Practices for Sustaining Accurate Facility Ratings

Extreme Weather Response

There were several notable extreme weather events in 2024 such as the Geomagnetic storm throughout the weekend of May 10 and Hurricane Beryl and its impacts to Texas. As noted in the 2023 Long-Term Reliability Assessment, recent extreme winter weather has exposed vulnerabilities to generating units and fuel sources that are not adapted to cold temperatures, raising concerns for blackstart unit readiness. The changing resource mix is cause for additional awareness of blackstart capabilities. Currently, few IBRs on the system are capable of grid forming control, one of the necessary components for blackstart resources.[29] Cold weather events can stress the BPS and expose weaknesses such as poor coordination between neighboring entities in planning or operations.

Geomagnetic disturbance events (GMD) are also a rising concern as the BPS footprint expands. The Earth has experienced a G5, or extreme geomagnetic storm in early 2024. G5 is the highest level on the five-step scale used by the National Oceanic and Atmospheric Administration (NOAA) to assess the strength of solar storms. It was the strongest solar storm to hit Earth since 2003.[30] "Power grid operators were busy working to keep proper, regulated current flowing without disruption," said Shawn Dahl, service coordinator for the Boulder, Co.-based Space Weather Prediction Center at NOAA.[31]

In 2023 and May of 2024, 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 Reliability 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.

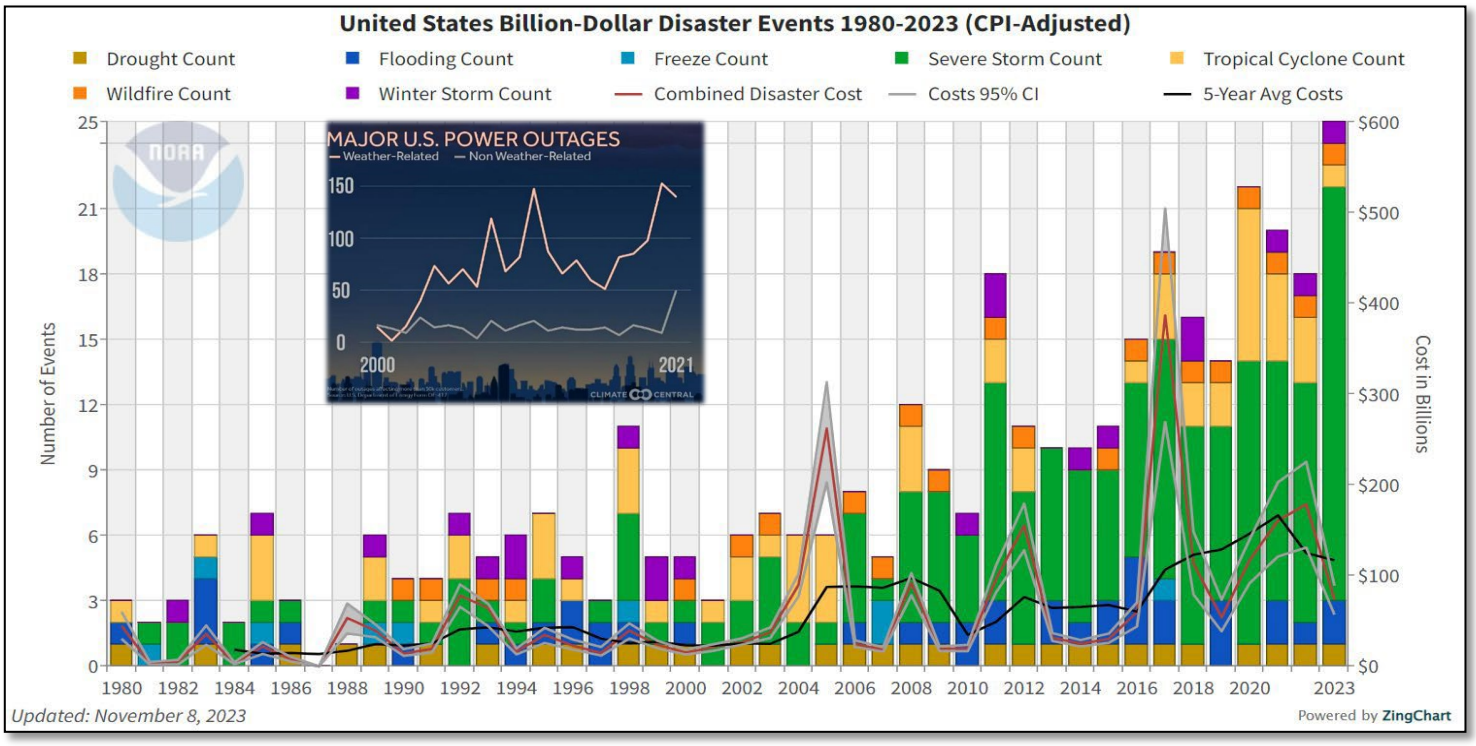
As severe weather increases the frequency of power outages, causes supply chain delays, amplifies impacts from personnel shortages, damages larger areas causing prolonged restoration times, negative impacts will increase for key security personnel and necessary physical security systems.[32] As displayed in the graphic below, between 2000 and

2021, about 83% of reported major outages in the U.S. were attributed to weather related events. For instance, severe hailstorms can damage renewables like wind turbines and solar power.

- The average annual number of weather-related power outages increased by roughly 78% during 2011-2021, compared to 2000-2010.
- The decade from 2011-2021 experienced 64% more major power outages than that from 2000-2010. From 2000-2021, there were 1,542 weather-related power outages nationally.
- Most outages were caused by severe weather (58%), winter weather (22%), and tropical cyclones (15%). These events are all likely to increase damage caused and duration of outages to rise.

[29] 2023 Long-Term Reliability Assessment(nerc.com)
[30] May solar superstorm caused largest 'mass migration' of satellites in history | Space
[31] The giant solar storm is having measurable effects on Earth : NPR
[32] CISA Extreme Weather Outreach (nerc.com)

- Wind turbines/solar panels exposed to freeze events or extreme icing may see significant output loss.
- Drought: In 2021-2022 the Upper Missouri River saw numerous hydroelectric plants shutdown earlier than normal due to low water levels.[33]



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 each Transmission Operator and Balancing Authority has developed plan(s) to mitigate operating Emergencies	EOP-011-4 (effective date TBD)	R1, R2, R3, R6	Balancing Authority Reliability Coordinator Transmission Operator Distribution Provider* UFLS-Only Distribution Provider* Transmission Owner* *Identified in the Transmission Operator's Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area

[33] CISA Extreme Weather Outreach (nerc.com)

Ensure each Generator Owner has developed and implemented plan(s) to mitigate the reliability impacts of extreme cold weather	EOP-012-2	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 Transmission Owner Generator Owner

Revision History

Version	Date	Revision Detail
Version 1.0		• Release of the 2025 ERO CMEP Implementation Plan.
Version 2.0	11/7/2024	• Updated PDS Schedule information