NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2023 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 1.0

October 2022

RELIABILITY | RESILIENCE | SECURITY




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

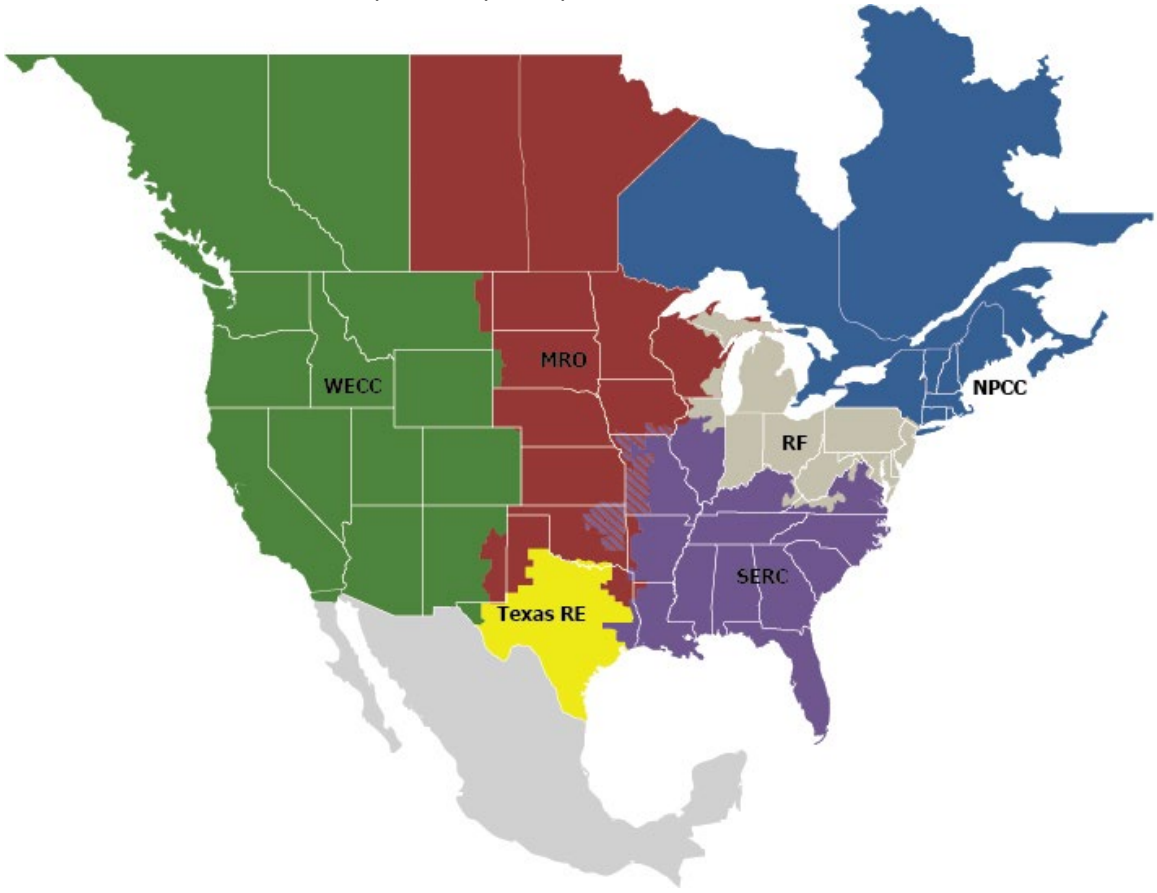
Table of Contents

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.



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 2022	• Release of the 2023 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 2023 CMEP IP describing the risks that will be priorities for the ERO Enterprise's CMEP activities in 2023. 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 our monitoring and enforcement efforts in 2023 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. 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, Appendix 4C Section 3.0 (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 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 and 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.

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

Documents	Year	Category	Date
Compliance (36)			
CIP ERT & User Guide (3)			
CIP FAQs (1)			
Compliance (10)			
2022 ERO Enterprise Periodic Data Submittal Schedule	2022	Compliance	12/16/2021
2023 ERO Enterprise Periodic Data Submittal Schedule	2023	Compliance	10/14/2022

2023 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 2022 risk elements to determine applicability for 2023. 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 2023 risk elements included in Table 2 reflect the continued maturation of the risk-based approach to compliance monitoring. The names of the Risk Elements have been changed from previous years, and the content of them made more direct, more specifically reflecting the discrete risks that may receive increased focus from CMEP staff. Even though there are more risk elements, they are targeted. 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.

The resulting risk elements are shown in Table 1. The 2022 risk element "models impacting long-term and operational planning" was refocused on specific concerns, namely into the new risk elements named "stability studies" and "inverter-based resources". The 2022 risk element "gaps in program execution" was retired as being too broad of a topic, and "protection system coordination" was merged into "inverter-based resources". Meanwhile, the 2022 risk element "extreme events" has been focused into "cold weather response" and "incident response". The risk elements "remote connectivity" and "supply chain" remain largely the same as they were already focused on particular risks.

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

[5] RISC ERO Priorities Report; August 2021

[6] NERC State of Reliability 2022

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 Q4 2022, the ERO Enterprise released the ERO Enterprise Themes and Best Practices for Sustaining Accurate Facility Ratings report [7] intended to aid stakeholders in strengthening the accuracy and sustainability of their facility ratings programs, resulting in the lessening of facility ratings challenges and ensuring a more reliable and secure bulk power system. To support our stakeholders, the ERO Enterprise actively engaged in mitigating activities associated with facility ratings and identified four common themes that pose challenges to the sustainability of accurate facility ratings:

- Lack of awareness
- Inadequate asset and data management
- Inadequate change management
- Inconsistent development and application of facility ratings methodologies

Table 1: 2022 Risk Elements
Remote Connectivity
Supply Chain
Models Impacting Long-term and Operational Planning
Gaps in Program Execution
Protection System Coordination
Extreme Events

Table 2: 2023 Risk Elements
Remote Connectivity
Supply Chain
Incident Response
Stability Studies
Inverter-Based Resources
Facility Ratings
Cold Weather Response

[7] ERO Enterprise Themes and Best Practices for Sustaining Accurate FR - Final - Oct-20-22.pdf (nerc.com)

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 2021 RISC report[9] continues to emphasize the need to control poor cyber hygiene. The 2022 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 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) 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 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. [11]

Areas of Focus

Table 3: Remote Connectivity

Rationale	Standard	Req	Entities for	Asset Types
Remote access to Critical Infrastructure Cyber Assets introducing increased attack surface, as well as possible increased exposure.	CIP-005-7	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission 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	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission Facilities Substations

[8] ERO Reliability Risk Priorities; February 2018

[9] RISC ERO Priorities Report; November 2021

[10] 2022 State of Reliability report

[11] US-CERT TA18-074A

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]

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 an 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.

[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

[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

Area of Focus

Table 4: Supply Chain				
Rationale	**Standard**	**Req**	**Entities for**	**Asset Types**
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	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission Facilities Substations
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	Backup Control Centers Control Centers Data Centers Generation Facilities Transmission Facilities Substations

Incident Response

Incident response has increasingly emerged as a risk to the BPS. Dragos has published a white paper[22] on the malware developed by threat group Chernovite named Pipedream. This particular piece of malware is targeting 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.

Area of Focus

Table 5: Incident Response				
Focused Risk	**Standard**	**Req**	**Entities for**	**Asset Types**
Mitigate risks to the reliable operation of the BES as the result of a Cyber Security Incident.	CIP-008-6	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 Transmission Facilities Substations

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

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 2021 Long-term Reliability Assessment highlights BPS risks associated with inverter-based resources (IBRs).[23] 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 grid transformation impacts.[24] 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.

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 in order 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 be 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	Requirements	Entities for Attention
Planning studies are effective in identifying system performanc e issues following both minor and major system disturbances	TPL-001-4, TPL-001-5.1	R4, R6	Transmission Planner Planning Coordinator
	CIP-014-3	R1	Transmission Owner

[23] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2021.pdf

[24] https://www.nerc.com/comm/RSTC/Pages/default.aspx

Inverter-Based Resources

Studies have shown a need to understand and more accurately model IBR characteristics. NERC has identified adverse characteristics of IBRs in two separate Alerts.[25,26] NERC has also released detailed reports about disturbances in Texas[27] and California[28] 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 this within their models.[29]

The Texas[30] and California[31] 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.[32]

For transparency, NERC's Inverter-Based Resource Strategy was released in September 2022[33].

Area of Focus

Table 7: Inverter-Based Resources

Rationale	Standard	Requirements	Entities for Attention
Clear and consistent interconnection requirements for IBRs	FAC-001-3	R1, R2	Generator Owner Transmission Owner
IBRs being adequately studied	FAC-002-3	R1, R2	Generator Owner Transmission Planner Planning Coordinator
IBRs staying online when needed	PRC-024-3	R1, R2	Generator Owner

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

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

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

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

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

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

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

[32] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/ERO%20Enterprise%20CMEP%20Practice%20Guide%20Regarding%20Inverter-Based%20Resources.pdf

[33] https://www.nerc.com/comm/Documents/NERC_IBR_Strategy.pdf

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 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 is 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.

Table 8: Facility Ratings

Rationale	Standard	Requirements	Entities for Attention
Ensuring entities maintain accurate Facility Ratings	FAC-008-5	R6	Generator Owner Transmission Owner

Cold Weather Response

Cold weather events encompass a wide range of situations that can cause major BPS impacts. As identified in the 2021 RISC report,[34] recent cold weather events (e.g., in ERCOT, MISO, and SPP) show that not only do 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.

This risk element needs to be understood in light of: the recently expedited FERC approval[35] of the Cold Weather Reliability Standards,[36] 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,[37] and the *Cold Weather Preparations for Extreme Weather*[38] *Events* Alert.[39] 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. The ERO Enterprise has developed a Practice Guide[40] to support understanding of this risk.

Areas of Focus

Table 9: Cold Weather Response

Rationale	Standard	Requirements	Entities for Attention
Ensure plans are developed and implemented to mitigate operating Emergencies	EOP-011-2	R1, R2, R3, R6, R7	Balancing Authority Generator Owner Reliability Coordinator Transmission Operator

[34] RISC ERO Priorities Report; August 2021

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

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

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

[38] 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.

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

[40] ERO Enterprise CMEP Practice Guide - Cold Weather Preparedness