

**NERC**

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# 2021 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 2.0

November 2020

RELIABILITY | RESILIENCE | SECURITY



3353 Peachtree Road NE  
Suite 600, North Tower  
Atlanta, GA 30326  
404-446-2560 | [www.nerc.com](http://www.nerc.com)

# Table of Contents

---

|   |     |
|---|-----|
| Preface .....   | iii |
| Revision History.....   | iv  |
| Introduction .....  | 1   |
| Purpose.....  | 1   |
| Monitoring Schedules.....   | 1   |
| Periodic Data Submittals .....                                      | 2   |
| 2021 ERO Enterprise Risk Elements .....                             | 3   |
| Process for Risk Elements and Associated Areas of Focus .....       | 3   |
| Pandemic Effects on CMEP Activities .....                           | 3   |
| Impact of Risk Elements.....  | 3   |
| Remote Connectivity and Supply Chain.....                           | 5   |
| Poor Quality Models Impacting Planning and Operations .....         | 7   |
| Loss of Major Transmission Equipment with Extended Lead Times ..... | 8   |
| Inadequate Real-time Analysis during Tool and Data Outages .....    | 9   |
| Determination and Prevention of Misoperations .....                 | 11  |
| Gaps in Program Execution.....                                      | 12  |

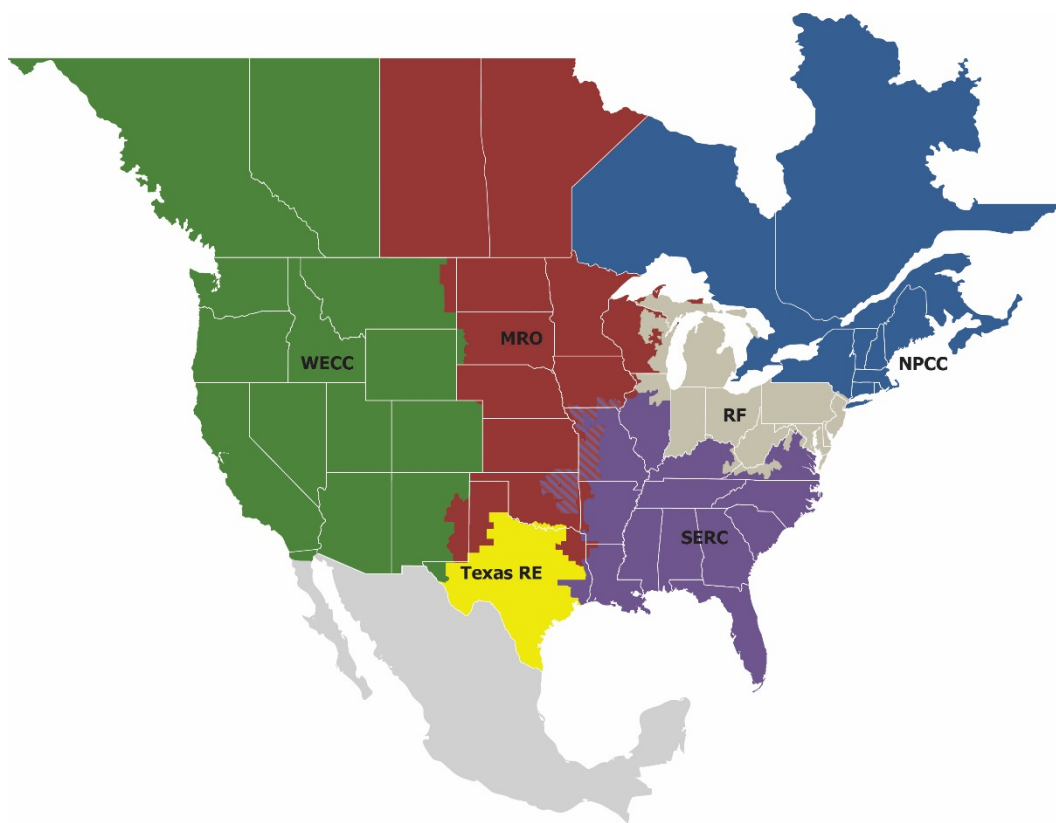
# Preface

---

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

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

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



|                 |  |
|-----------------|--|
| <b>MRO</b>      | Midwest Reliability Organization         |
| <b>NPCC</b>     | Northeast Power Coordinating Council     |
| <b>RF</b>       | ReliabilityFirst                         |
| <b>SERC</b>     | SERC Reliability Corporation             |
| <b>Texas RE</b> | Texas Reliability Entity                 |
| <b>WECC</b>     | Western Electricity Coordinating Council |

## Revision History

---

| Version     | Date          | Revision Detail   |
|-------------|---------------|---|
| Version 1.0 | October 2020  | <ul style="list-style-type: none"><li>• Release of the 2021 ERO CMEP Implementation Plan.</li></ul> |
| Version 2.0 | November 2020 | <ul style="list-style-type: none"><li>• Added links to monitoring schedules.</li></ul>              |

# Introduction

---

## Purpose

The Electric Reliability Organization (ERO) Enterprise<sup>1</sup> 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.<sup>2</sup>

The ERO Enterprise is pleased to release the 2021 CMEP IP using the enhanced, easier to use format introduced in the 2020 CMEP IP. Collectively, NERC and each RE have worked collaboratively throughout this IP's development to streamline the ROP's timing and risk assessment processes into one cohesive narrative, compared to a main IP with several regional appendices as in years past. By streamlining the development in this manner, the ERO Enterprise is also more effectively and efficiently fulfilling the timing and risk assessment obligations of the CMEP IP.

Through this enhancement, the ERO Enterprise will address areas where there may be specific regional considerations in the main risk element description. This will provide a more user-friendly and relevant IP to registered entities. Specifically, the IP represents the ERO Enterprise's high-level priorities for its CMEP. 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 internal controls and compliance operations focus.

## Monitoring Schedules

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

- MRO: [MRO Compliance Audits Tools and Resources](#)
- NPCC: [NPCC Audit Schedules](#)
- ReliabilityFirst: [ReliabilityFirst Compliance Monitoring Page \(see Schedules\)](#)
- SERC: [SERC 2021 CMEP IP](#)
- Texas RE: [Texas RE 2021 Annual Audit Plan](#)
- WECC: [2021 WECC US Audit Schedule](#)

---

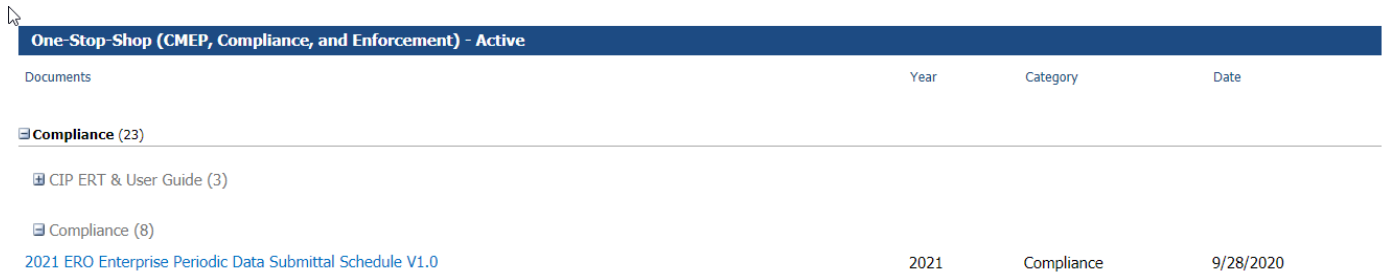
<sup>1</sup> The ERO Enterprise comprised of NERC and the six Regional Entities, which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the ERO's statutory obligations to assure the reliability of the North American BPS.

<sup>2</sup> [NERC ROP](#), Appendix 4C Section 4.0 (Annual Implementation Plans).

## Periodic Data Submittals

The Compliance Enforcement Authority (CEA) requires 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 Rules of Procedure (RoP), Appendix 4C Section 3.6.

The Regional Entities use the periodic data submittal schedule<sup>3</sup> posted by NERC on the NERC Compliance One-Stop Shop, located under “Compliance” at this link: [NERC Compliance One-Stop Shop](#)



| Documents   | Year | Category   | Date      |
|---|------|------------|-----------|
| <b>Compliance (23)</b>  |      |            |           |
| CIP ERT & User Guide (3)  |      |            |           |
| Compliance (8)  |      |            |           |
| <a href="#">2021 ERO Enterprise Periodic Data Submittal Schedule V1.0</a> | 2021 | Compliance | 9/28/2020 |

<sup>3</sup> In addition, WECC has two WECC Criterion on which it collects data annually ([2021 WECC Periodic Data Submittal Schedule](#)).

## 2021 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.<sup>4</sup> As such, the ERO Enterprise identifies risk elements using data including, but not limited to: compliance findings; event analysis experience; data analysis; and the expert judgment of ERO Enterprise staff, committees, and subcommittees (e.g., NERC's Reliability Issues Steering Committee or RISC). Reviewed publications include the RISC's biennial report,<sup>5</sup> the State of Reliability Report,<sup>6</sup> the Long-Term Reliability Assessment, publications from the RISC, special assessments, the ERO Enterprise Strategic Plan, and ERO Event Analysis Process insights. The ERO Enterprise uses these risk elements to identify and to prioritize interconnection and continent-wide risks to the reliability of the BPS. These identified risks are used to focus compliance monitoring and enforcement activities.

The ERO Enterprise reviewed and reassessed the 2020 risk elements to determine applicability for 2021. The 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 REs will develop an informed list of NERC Reliability Standards and Requirements for any monitoring activities specific to a registered entity's risks. Notably, the IP is not intended to be a representation of just "important" Reliability Standard requirements; rather, it is intended to reflect the ERO Enterprise's prioritization within its CMEP based on its inputs and to communicate to registered entities to bring collective focus within their operations to address each prioritized risk.

### Pandemic Effects on CMEP Activities

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

In May 2020, the ERO Enterprise released guidance<sup>7</sup> which provided additional regulatory relief related to registered entities' coronavirus response and temporarily expanded the Self-Logging Program. Due to the ongoing pandemic, the ERO Enterprise extended this expansion through December 31, 2020, to allow all registered entities to self-log instances of potential noncompliance with minimal or moderate risk related to their coronavirus response.

During 2021, the ERO Enterprise recognizes the importance of prioritizing the health and safety of personnel and the continued reliability and security of the bulk power system. We will evaluate the circumstances to determine the need for additional guidance or extensions. When conditions allow, the ERO Enterprise will prioritize monitoring activities and risks that benefit the most from on-site components, including some on-site activities deferred from 2020.

### Impact of Risk Elements

The REs evaluate the relevancy 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.

---

<sup>4</sup> Appendix C, [ERO Enterprise Guide for Compliance Monitoring; October 2016](#)

<sup>5</sup> [RISC ERO Priorities Report; November 2019](#)

<sup>6</sup> [NERC State of Reliability 2019](#)

<sup>7</sup> [ERO Enterprise Releases New Guidance Temporarily Expanding Self-Logging Program Due to Coronavirus Impacts](#)

The 2021 risk elements are included in Table 1 below and reflect the maturation of the risk-based approach to compliance monitoring from 2020. As the ERO Enterprise and industry continue to become more knowledgeable about the risks that require control emphasis or mitigation, risk elements will focus more on discrete risks. These discrete risks provide focus for measuring current state and validating registered entity progress. By tracking improvements, industry and the ERO Enterprise can justify focusing on different risks in the future.

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

The COVID-19 pandemic has caused some risks to BPS Operations and the risk element write ups have been updated slightly from 2020 to reflect some of these concerns. The risk from potential pandemics has been considered in years past as well as 2021. As identified in NERC's Preparedness and Operational Assessment published in Spring 2020,<sup>9</sup> pandemic risk differs from many of the other threats facing the BPS because it is a "people event." The fundamental risk is the loss of staff critical to operating and maintaining the BPS such that firm loads could no longer be served reliably and securely. Regions may consider reviewing requirements related to personnel training in order to address this risk.

---

<sup>8</sup>For example, in 2019, the ERO Enterprise noted in its 2019 CMEP IP that it may engage in targeted efforts to understand entities implementation of specific, newer aspects of IRO-008 and TOP-001. NERC, RE, and FERC staff worked in 2019 to better understand the strategies and techniques used by entities to perform Real-time Assessments (RTAs) during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the Regional Entities (REs) began collaborating with a small number of entities to focus on the practices and controls to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001). Aggregated information on potential industry best practices and concerns will be outlined in a public report after completion of the activity, which is expected in 2021.

<sup>9</sup>[https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_Pandemic\\_Preparedness\\_and\\_Op\\_Assessment\\_Spring\\_2020.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Pandemic_Preparedness_and_Op_Assessment_Spring_2020.pdf)



**Table 1: Comparison of 2020 Risk Elements and 2021 Risk Elements**

| 2020 Risk Elements  | 2021 Risk Elements  |
|---|---|
| Management of Access and Access Controls                                | Remote Connectivity and Supply Chain                          |
| Insufficient Long-Term and Operations Planning Due to Inadequate Models | Poor Quality Models Impacting Planning and Operations         |
| Loss of Major Transmission Equipment with Extended Lead Times           | Loss of Major Transmission Equipment with Extended Lead Times |
| Inadequate Real-time Analysis During Tool and Data Outages              | Inadequate Real-time Analysis During Tool and Data Outages    |
| Improper Determination of Misoperations                                 | Determination and Prevention of Misoperations                 |
| Gaps in Program Execution   | Gaps in Program Execution                                     |
| Texas RE: Resource Adequacy   |   |

### Remote Connectivity and Supply Chain

The protection of critical infrastructure remains an area of significant importance. This risk element focuses on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.<sup>10</sup> The 2019 RISC report<sup>11</sup> continues to emphasize the need to control poor cyber hygiene. The 2019 State of Reliability report<sup>12</sup> highlights trusted third-party phishing, crypto-jacking and ransomware, and malware frameworks as the most prominent cyber security threats. One of the effects of COVID-19 has been changes to the designed interaction between employees and their workspaces which could have unintended effects on the controls in place to protect critical infrastructure.

Regardless of the sophistication of a security system, there is potential for human error. Compliance monitoring should seek to understand how entities manage the risk of remote connectivity and the complexity of the tasks the individuals perform. If security has increased the difficulty in performing personnel's normal tasks, personnel may look for ways to circumvent the security to make it easier to perform their job. On the other hand, when an entity replaces complex tasks with automation, focus should be on: 1) whether the automation was correctly configured; 2) controls to ensure the automation is operating as intended; and 3) how access, the ability to obtain and use, is implemented.

Harvesting credentials and exploiting physical and logical access of authorized users of BES facilities and Cyber Systems (BCSs) pose a major risk to systems that monitor and control the BES. With the target being users, privileged or non-privileged, who have authorized unescorted physical access and/or various levels of access to critical elements of the BES, the risk becomes elevated. By actively and covertly employing social engineering techniques and phishing emails, attackers may deceive authorized users to harvest credentials and gain unauthorized access.<sup>13</sup>

<sup>10</sup> [ERO Reliability Risk Priorities; February 2018](#)

<sup>11</sup> [RISC ERO Priorities Report; November 2019](#)

<sup>12</sup> [2019 State of Reliability report](#)

<sup>13</sup> [US-CERT TA18-074A](#)

Supply Chain risk is growing and is continuing to be a focal point of the federal government. With FERC releasing numerous Notice of Inquiries<sup>14</sup> that sought information on supply chain vulnerabilities, along with the Presidential Executive Order<sup>15</sup> banning Huawei manufacturer equipment, supply chain risk from international espionage is only increasing. NERC has published NERC Alerts on this topic<sup>16</sup>. Various publications have highlighted several vendors, services, and products widely utilized by industry underscoring the importance of awareness as it relates to the supply chain risks<sup>17</sup>. Additionally, it has been reported that security components of BES Cyber Systems have been compromised within their respective supply chains<sup>18</sup>. While these risks can create issues within individual entities, collectively they could cause disruptions within the BES.

**Areas of Focus**

| <b>Table 2: Remote Connectivity and Supply Chain</b> |                    |   |  |
|--|--------------------|---|--|
| <b>Standard</b>                                      | <b>Requirement</b> | <b>Entities for Attention</b>   | <b>Asset Types</b>   |
| CIP-005-6  | R2                 | Balancing Authority<br>Distribution Provider<br>Generator Operator<br>Generator Owner<br>Reliability Coordinator<br>Transmission Operator<br>Transmission Owner | Back up Control Centers<br>Control Centers<br>Data Centers<br>Generation Facilities<br>Substations |
| CIP-007-6  | R1                 | Balancing Authority<br>Distribution Provider<br>Generator Operator<br>Generator Owner<br>Reliability Coordinator<br>Transmission Operator<br>Transmission Owner | Backup Control Centers<br>Control Centers<br>Data Centers<br>Generation Facilities<br>Substations  |
| CIP-010-3  | R1                 | Balancing Authority<br>Distribution Provider<br>Generator Operator<br>Generator Owner<br>Reliability Coordinator<br>Transmission Operator<br>Transmission Owner | Backup Control Centers<br>Control Centers<br>Data Centers<br>Generation Facilities<br>Substations  |
| CIP-013-1  | R1, R2             | Balancing Authority<br>Distribution Provider<br>Generator Operator<br>Generator Owner<br>Reliability Coordinator<br>Transmission Operator<br>Transmission Owner |  |

<sup>14</sup> [Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security; Potential Enhancements to the Critical Infrastructure Protection Reliability Standards](#) and [Virtualization and Cloud Computing Services](#)

<sup>15</sup> [Executive Order on Securing the Information and Communications Technology and Services Supply Chain](#)

<sup>16</sup> [NERC Alerts](#)

<sup>17</sup> [EPRI Supply Chain Risk Assessment Report; July 2018](#)

<sup>18</sup> [NATF Cyber Security Supply Chain Risk Management Guidance; June 2018](#)

## Poor Quality Models Impacting Planning and Operations

Long-term and Operational Planning are performed for the integration and management of system assets. This includes system analyses of other emerging issues and trends (e.g., significant changes to the use of demand-side management programs, the integration of inverter-based resources and variable energy resources, changes in load characteristics, increasing dependence on natural gas deliverability for gas-fired generation, increasing uncertainty in nuclear generation retirements, and essential reliability services). NERC's annual Long-Term Reliability Assessment<sup>19</sup> forms the basis of NERC's assessment of emerging issues to BPS reliability. The ERO continues to raise awareness on inverter-based resource performance through NERC alerts<sup>20</sup> and industry outreach. Compliance monitoring should seek to understand how entities adapt to new practices and tools to mitigate emerging risks in this continually changing environment.

Inadequate long-term planning can lead to increased risks to reliability. Accurately modeled planning cases become increasingly critical as a changing resource mix, deployment of new technologies, etc., affect the risk to BPS reliability. For instance, models should reflect if power electronic controls of utility-scale inverter-based resources, such as PV resources, enable both real and reactive power generation. As stated in the NERC 2020 State of Reliability report, "Planners and operators may be challenged to integrate these inputs and will need to make necessary changes, such as revising operational practices and procedures, enhancing NERC Reliability Standards, or changing market designs."<sup>21</sup> The 2019 RISC report<sup>22</sup> states that *"the continued integration of large amounts of new resource technologies (e.g., DERs, grid and distribution system-connected inverter-based resources, and energy storage) could lead to inaccurate forecasting of anticipated demand. Further, this integration can also result in other planning and operational challenges if these resource additions are not observable or predictable or are otherwise not taken into account. The dynamic and transient performance and response of these technologies also brings new challenges."* In addition, enhancements to models will be needed to support probabilistic analysis to accommodate the energy limitations of resource additions (such as variable renewable resources). Resource adequacy must look beyond the calculation of reserve margins that assume actual capacity available during peak hours.

Insufficient operational planning can lead to increased risks to reliability in the near-term. Comprehensive dynamic load models will be needed to sufficiently incorporate behind-the-meter generation and distributed load resources such as demand-side management programs. One of the ways in which the industry can better understand the system is by monitoring load characteristics and the changing nature of load due to Distributed Energy Resources (DER). The NERC Load Modeling Task Force developed a reliability guideline that provides Transmission Planners and Transmission Owners with insights into end-use load behaviors and how to capture them in the composition of dynamic load models.<sup>23</sup> Additionally, the 2020 NERC-WECC Joint Report<sup>24</sup> regarding inverter-based resources in the Western Interconnection base case found "many different findings and takeaways on modeling issues identified in the steady-state power flow base case and associated dynamics data records." Industry is encouraged to consider recommendations from that report for their own footprint and model needs.

---

<sup>19</sup> [NERC Long-Term Reliability Assessment 2019](#)

<sup>20</sup> <https://www.nerc.com/news/Documents/Inverter%20Alert%20Announcement.pdf>

<sup>21</sup> [https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC\\_SOR\\_2020.pdf](https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf)

<sup>22</sup> [RISC ERO Priorities Report; November 2019](#)

<sup>23</sup> [NERC Modeling Improvements Initiative Update; May 2018](#)

<sup>24</sup> [NERC-WECC Joint Report: WECC Base Case Review: Inverter-Based Resources; August 2020](#)

In order to achieve performance expected by the planning models, generating plant protection schemes and their settings should be coordinated with transmission protection, control systems, and system conditions to minimize unnecessary trips of generation during system disturbances.<sup>25</sup>

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

Additional studies have similarly shown a need to understand and more accurately model inverter-based resource characteristics. NERC has identified adverse characteristics of inverter-based resources in two separate Alerts.<sup>26,27</sup> With the recent and expected increases of both utility-scale solar resources and distributed generation, the causes of a sudden reduction in power output from utility-scale power inverters needs to be widely communicated and addressed by the industry. Entities with increasing inverter-based resources should be aware and address this within their models.<sup>28</sup>

*Areas of Focus*

| Table 3: Poor Quality Models Impacting Planning and Operations |              |  |                                      |
|--|--------------|--|--------------------------------------|
| Standard   | Requirements | Entities for Attention   | Rationale                            |
| MOD-026-1  | R2           | Generator Owner<br>Transmission Planner  | Ensure adequate models of generation |
| MOD-027-1  | R2           | Generator Owner<br>Transmission Planner  | Ensure adequate models of generation |
| MOD-033-1  | R1, R2       | Planning Coordinator<br>Reliability<br>Coordinator<br>Transmission<br>Operator | Ensure accurate System models.       |

**Loss of Major Transmission Equipment with Extended Lead Times**

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

<sup>25</sup> [Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings; June 2017](#)

<sup>26</sup> [Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings - II; May 2018](#)

<sup>27</sup> [NERC Modeling Notification: Recommended Practices for Modeling Momentary Cessation Distribution; February 2018](#)

<sup>28</sup> [Considerations for Power Plant and Transmission System Protection Coordination, July 2015](#)

These scenarios include:

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

As the BPS ages, less-than-adequate infrastructure maintenance is a reliability risk that continues to grow. The RISC report identifies that the failure to maintain equipment is a reliability risk exacerbated when an entity either does not have replacement components available or cannot procure needed parts in a timely fashion. The failure to properly commission, operate, maintain, prudently replace, and upgrade BPS assets generally could result in more frequent and wider-spread outages, and these could be initiated or exacerbated by equipment failures.

An entity’s awareness of its Facilities that have extended replacement lead times can affect real-time operations. In some cases, pre-emptive actions may be needed to protect identified major transmission equipment with extended lead times. As noted in the 2019 RISC Report: “Wild Fires can be a direct threat to BES equipment. Pre-emptive actions must be taken to de-energize equipment without causing additional cascading effects in areas where wild fire risk is significant.”<sup>29</sup>

Spare equipment strategy is an important aspect of restoration and recovery. The strategy and its related controls should encompass identifying critical spare equipment as part of a national or regional inventory. For example, as part of the changing resource mix supplying power to the BPS, Blackstart units may be retired; as a result, the remaining Blackstart units become more critical to ensure proper and timely system recovery. The strategy should also account for the transportation and logistics requirements for replacing critical assets. An improved spare equipment strategy or plan will lead to better contingency planning and possibly faster response times for restoration and recovery. A spare equipment strategy can help strengthen the resiliency for responding to potential physical threats and vulnerabilities.<sup>30</sup>

**Areas of Focus**

| Table 4: Loss of Major Transmission Equipment with Extended Lead Times |              |  |  |
|--|--------------|--|--|
| Standard   | Requirements | Entities for Attention                       | Rationale  |
| TPL-001-4  | R2.1.5       | Planning Coordinator<br>Transmission Planner | Ensure that unavailability of major Transmission equipment has been considered in the entity’s spare equipment strategy. |

**Inadequate Real-time Analysis during Tool and Data Outages**

Without accurate tools and data, operators may not make decisions that are appropriate to ensure reliability for the actual state of the system. NERC’s ERO Top Priority Reliability Risks 2014-2017 notes that “stale” data and lack of analysis capabilities contributed to the blackout events in 2003 (“August 14, 2003 Blackout”) and 2011 (“Arizona-

<sup>29</sup> [RISC ERO Priorities Report; November 2019](#)

<sup>30</sup> [CIP-014-2 Guidelines and Technical Basis, Requirement R5](#)

Southern California Outages”). Essential primary and alternate capabilities must be in place with up-to-date information available for staff to use on a regular basis to make informed decisions.

Specifically, entities are encouraged to have realistic plans to continue real-time analyses such as those performed for the Real-time Assessment (RTA) during outages of tools, loss of data, or both. The 2019 RISC report<sup>31</sup> identifies that “loss or degradation of situational awareness poses BPS challenges as it affects the ability of personnel or automatic control systems to perceive and anticipate degradation of system reliability and take pre-emptive action.” This risk element is more challenging in situations where planning models may not keep pace with increasing complexity of newer technologies impacting generation or load characteristics.

Registered entities should be able to demonstrate how their Real-time Assessment is sufficient during normal operations as well as during the loss of primary tools or data sources. Efforts should be made by registered entities to ensure data quality is measured and tracked for feedback into continual data quality improvements. Alternate practices and tools for conducting a sufficient RTA must be in place and periodically trained to by the entity’s System Operators, EMS support teams, or other impacted staff.

This risk element will continue to be evaluated pending the results of ongoing activities. The ERO Enterprise and FERC staff have sought to better understand the strategies and techniques used by entities to perform RTAs during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the Regional Entities (REs) collaborated with a nine volunteer entities in 2019 to focus on RTA practices and controls. Additionally, the team sought to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001). Aggregated information on potential industry best practices and concerns will be outlined in a public report in 2021.

The 2020 NERC State of Reliability report<sup>32</sup> provides four recommendations:

- Electric utilities should develop and implement the system recovery and restoration plans, including scenarios in which the EMS and decision-support tools are unavailable. These plans should also include drills and training on the procedures plus real-life practice implementing the procedures.
- Electric utilities should use offline tools (studies) in addition to the real-time analysis tools in EMSs to analyze contingencies plus other contingency-analysis tools, including day-ahead studies as well as seasonal and standing operating guides; these contingency-analysis tools will provide a backup when the primary real-time analysis tools fail.
- Electric utilities should have backup tools and functionality ready and test them periodically. Backup tools and functionality include backup EMS systems, backup control centers, and other additional redundancy. The testing and use of these tools should be documented in emergency plans. System operators should be aware of these procedures and trained in using backup tools.
- Working with the ERO, electric utilities should develop and implement communication and response processes between RCs, BAs, and TOPs to improve overlapping coverage of situational awareness. The RCs, BAs, and TOPs should coordinate actions with their facilities to maintain the reliability of the BES.

---

<sup>31</sup> [RISC ERO Priorities Report; November 2019](#)

<sup>32</sup> [NERC State of Reliability 2020](#)

*Areas of Focus***Table 5: Inadequate Real-time Analysis during Tool and Data Outages**

| Standard  | Requirements | Entities for Attention  | Rationale  |
|-----------|--------------|-------------------------|--|
| IRO-008-2 | R4           | Reliability Coordinator | Ensuring situational awareness is maintained regardless of advanced applications which affect RTA status |
| TOP-001-4 | R13          | Transmission Operator   | Ensuring situational awareness is maintained regardless of advanced applications which affect RTA status |

**Determination and Prevention of Misoperations**

Protection systems are designed to remove equipment from service so the equipment will not be damaged when a fault occurs. Protection systems that trip unnecessarily can contribute significantly to the extent of an event. When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary. Such coordination errors occurred in the Arizona-Southern California Outages (see recommendation 19),<sup>33</sup> the August 14, 2003 Blackout (see recommendation 21),<sup>34</sup> and the Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015 (see recommendation 2).<sup>35</sup>

Furthermore, a protection system that does not trip—or is slow to trip—may lead to the damage of equipment (which may result in degraded reliability for an extended period of time), while a protection system that trips when it should not can remove important elements of the power system from service at times when they are needed most. Unnecessary trips or misoperations can even start cascading failures, as each successive trip can cause another protection system to trip. Thorough analysis of lessons learned from misoperations can have a substantial reliability impact.

The 2018 RISC report<sup>36</sup> includes a key point that the ERO Enterprise, the impacted organizations, and the respective forums and trade organizations should perform post-event reviews to capture lessons learned to reduce the impact of future events. These reviews will be incomplete if every event is not noticed because the relay operations were not reviewed by qualified personnel. The report also identifies the risk posed by the increasing complexity in protection and control systems, further emphasizing the importance of a skilled workforce analyzing events and relay operations. As identified in the NERC Preparedness and Operational Assessment Spring 2020<sup>37</sup>, pandemic risk differs from many of the other threats facing the BPS because it is a “people event.” As such, it is possible controls may be disrupted and unable to identify and correct these issues. Understanding how an entity uses controls can help promote best practices in this area.

<sup>33</sup> See [Arizona-Southern California Outages on September 8, 2011](#)

<sup>34</sup> See [Final Report on the August 14, 2003 Blackout](#)

<sup>35</sup> See [Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015](#)

<sup>36</sup> [ERO Reliability Risk Priorities; February 2018](#)

<sup>37</sup> [NERC Pandemic Preparedness and Op Assessment Spring 2020](#)

*Areas of Focus*

| <b>Table 6: Determination and Prevention of Misoperations</b> |                     |                                       |   |
|---|---------------------|---------------------------------------|---|
| <b>Standard</b>   | <b>Requirements</b> | <b>Entities for Attention</b>         | <b>Rationale</b>  |
| PRC-004-5(i)*   | R1, R5              | Generator Owner<br>Transmission Owner | Ensure proper analysis of protection system operations.       |
| PRC-027-1   | R1, R3              | Generator Owner<br>Transmission Owner | Ensure proper analysis of lessons learned from misoperations. |

**Gaps in Program Execution**

Effects of COVID-19 on the industry’s ability to mitigate risk are not completely apparent. Many controls have been set up to work a certain way under specific conditions. Registered entities need to understand the effects of changes to workspace, coworker interaction, coworker availability, resource availability, contractor availability, electronic access from alternate workspaces, and other adjustments. Monitoring focus on this area can help discover best practices in keeping existing controls working and effective, and in discovering what controls may need to be added.

As identified in the NERC Preparedness and Operational Assessment Spring 2020,<sup>38</sup> workforce availability constraints could extend the time necessary to respond to abnormal system conditions, troubleshoot and repair damaged facilities, preclude necessary preventive and corrective maintenance, prolong outage restoration, and possibly reduce reserve margins if generating facilities are forced offline.

COVID-19 has complicated registered entity inspection and maintenance programs because of travel limitations and physical distancing requirements. Vegetation management programs need to remain a priority for registered entities to reduce the risks of vegetation contacts.

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

<sup>38</sup> [https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC\\_Pandemic\\_Preparedness\\_and\\_Op\\_Assessment\\_Spring\\_2020.pdf](https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Pandemic_Preparedness_and_Op_Assessment_Spring_2020.pdf)



*Areas of Focus*

| <b>Table 7: Gaps in Program Execution</b> |                     |  |   |
|---|---------------------|--|---|
| <b>Standard</b>                           | <b>Requirements</b> | <b>Entities for Attention</b>  | <b>Rationale</b>  |
| CIP-010-3                                 | R1                  | Balancing Authority<br>Generator Owner<br>Transmission Operator<br>Transmission Owner<br>Reliability Coordinator | Ensuring entities maintain complex programs which handle large amounts of data, e.g., accurate inventories of equipment, following asset transfers, addition of new equipment, etc. |
| FAC-003-4                                 | R1, R2, R3, R6, R7  | Generator Owner<br>Transmission Owner  |   |
| FAC-008-3                                 | R6                  | Generator Owner<br>Transmission Owner  |   |
| PRC-005-6                                 | R3                  | Generator Owner<br>Transmission Owner  |   |