

Regional Risk Assessment

January 2025



**MIDWEST
RELIABILITY
ORGANIZATION**

Public

380 St. Peter St, Suite 800
Saint Paul, MN 55102

651-855-1760

MRO.net

TABLE OF CONTENTS

1. Preface	3
2. Executive Summary	4
About this Regional Risk Assessment	5
Key Assessment Findings	5
Summary of Top Regional Risks	6
Summary	7
3. Introduction	8
Industry Coordination and Collaboration	8
Inputs to the RRA Process	8
About the MRO Stakeholder Survey	9
Actions to Reduce Risks	9
Regional Risk Ranking Process	10
4. 2025 MRO Regional Risks and Rankings	12
Risk Prioritization Changes	13
Dormant Risks	15
Correlation of ERO-wide risks and MRO Regional Risks	15
5. Detailed Risk Information	18
Uncertain Energy Availability	19
Generation Outages During Extreme Cold Weather	23
Nation-State Threats	26
Supply Chain Compromise	30
Malicious Insider Threat	33
Inadequate IBR and DER Performance and Modeling	36
Phishing / Malware / Ransomware	39
Loss of Essential Reliability Services	42
Physical Attacks	44
Material and Equipment Availability	47
Internet-Connected Devices	49
Use of Inaccurate Transmission Facility Ratings	51
Tight Supply of Expert Labor	54
Vulnerabilities of Unpatched Systems	55
6. Conclusion	58
7. References	59



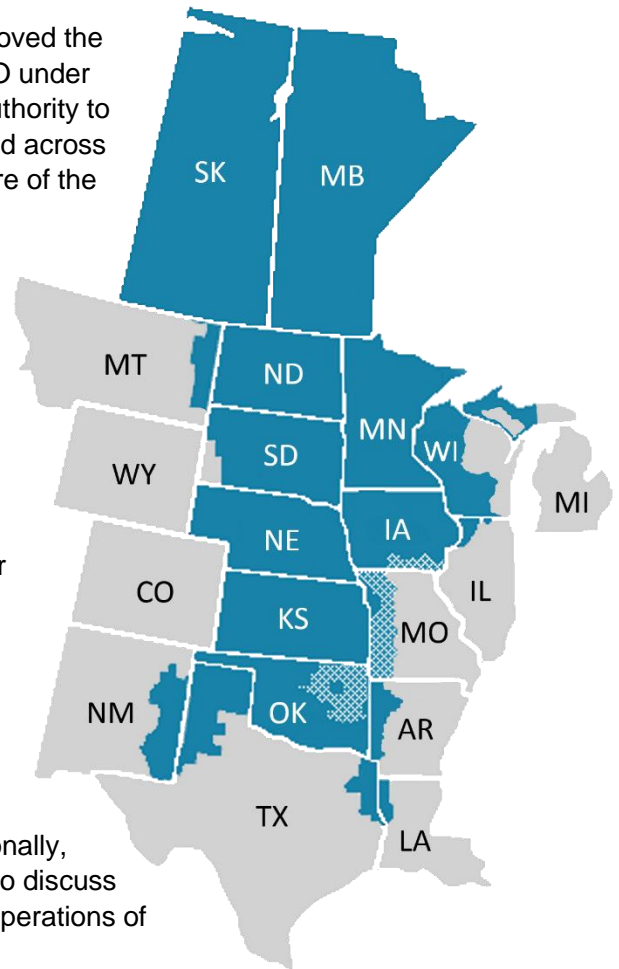
1. PREFACE

Midwest Reliability Organization (MRO) is dedicated to its vision of **a highly reliable and secure North American bulk power system**. To ensure reliability of the bulk power system in the United States, Congress passed the Energy Policy Act of 2005, creating a new regulatory organization called the Electric Reliability Organization (ERO) to establish mandatory Reliability Standards and monitor and enforce compliance with those standards on those who own, operate or use the interconnected power grid.

In 2006, the Federal Energy Regulatory Commission (FERC) approved the North American Electric Reliability Corporation (NERC) as the ERO under section 215(e)(4) of the Federal Power Act. NERC delegates its authority to monitor and enforce compliance to six Regional Entities established across North America, including MRO. Recognizing the international nature of the grid, NERC as the ERO, along with MRO, established similar arrangements with provincial authorities in Canada.

The MRO region spans the provinces of Saskatchewan and Manitoba, and all or parts of the states of Arkansas, Illinois, Iowa, Kansas, Louisiana, Michigan, Minnesota, Missouri, Montana, Nebraska, New Mexico, North Dakota, Oklahoma, South Dakota, Texas, and Wisconsin. The region includes approximately 245 organizations that participate in the production and delivery of electric power, including Canadian utilities, cooperative and municipal utilities, investor-owned utilities, along with federal power marketing agencies, generator power marketers, and transmission system operators.

MRO's primary responsibilities are to: monitor and enforce compliance with mandatory Reliability Standards by entities who own, operate, or use the North American bulk power system; conduct assessments of the grid's ability to meet electric power demand in the region; and analyze regional system events. Additionally, MRO creates an open forum for stakeholder experts in the region to discuss important topics related to addressing risk and improving reliable operations of the bulk power system.



2. EXECUTIVE SUMMARY

Within the MRO footprint, over 28 million people depend on a reliable electric grid to deliver electricity from where it is produced to where it is used. Demand for electricity is rapidly increasing. More and more sectors of the economy are relying on electricity to support new technology, reduce planet-warming emissions, and enrich people’s lives. At the same time, the way electricity is produced is undergoing a major transition, increasing the potential for system imbalances and making it harder to maintain a reliable power grid. Weather conditions are also having a greater impact on grid reliability. Not only is the supply and performance of some resources dependent on the weather, but extreme weather has become more prevalent and is necessitating enhanced system resiliency.

Protecting reliability and security of the regional power grid is the primary focus of MRO. We share an important mission with the ERO Enterprise to identify, prioritize, and assure the effective and efficient mitigation of risks to the reliability and security of the North American bulk power system. MRO’s annual Regional Risk Assessment (RRA or assessment) is an important part of achieving this mission. Our regional territory spans the middle part of North America from the Canadian provinces of Manitoba and Saskatchewan all the way down to Texas. We are uniquely situated at the intersection of three North American electric grids — the Western Interconnection, Eastern Interconnection, and Texas Interconnection (see Figure 1) — and provide a critical link to delivering diverse generating resources to customers within the region and beyond.

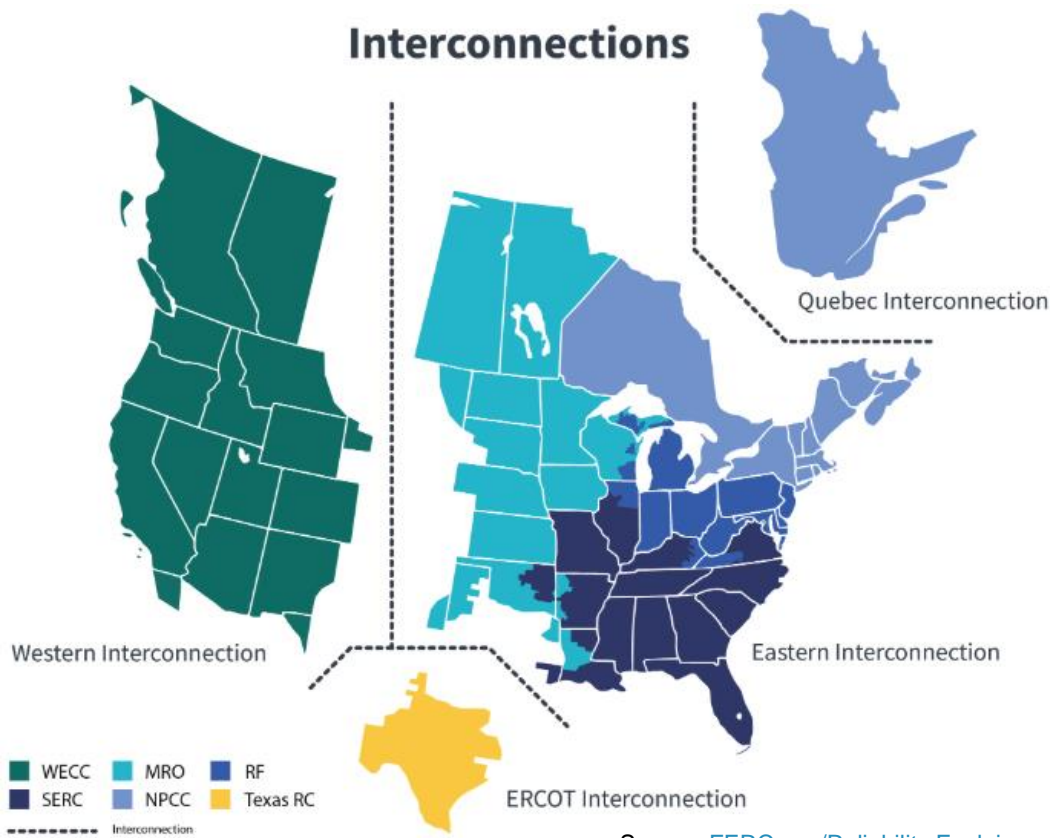


FIGURE 1 - NERC’S REGIONS AND ASSOCIATED INTERCONNECTIONS



About this Regional Risk Assessment

The RRA is developed collaboratively with industry experts that serve on MRO's Compliance Monitoring and Enforcement Program Advisory Council, Reliability Advisory Council, and Security Advisory Council. The assessment uses a variety of continent-wide and regional resources to identify the collective risks and trends challenging utilities within the region. The findings are then prioritized by a team of advisory council members and MRO staff based on the impact to reliability and security of the grid and likelihood of occurrence, the criteria for which were developed by the advisory councils in MRO's [reliability risk matrix](#).

Risk priority levels are categorized as *extreme*, *high*, *medium* or *low*. Extreme and high risks become the focus for regional efforts to raise awareness of risk and develop and implement mitigation activities.

Key Assessment Findings

A total of fourteen risks were identified in 2025, with six rising to an extreme or high priority. For the second year in a row, *Uncertain Energy Availability* landed as the top risk to reliability of the regional bulk power system and the only extreme risk in this assessment. It is important to note that the extreme risk designation was given because of the North American-wide impact and likely occurrence of this risk, which is described in more detail in this report.

Five other risks were identified as high priority in this assessment. While four of the five are consistent with previous risk assessments, *Nation-State Threats* is a new risk designated in the high category because of the current geopolitical climate. Table 1 lists the extreme and high risks in priority order from highest to lowest.

Table 1: Top Regional Risks	
Risk	Priority
Uncertain Energy Availability	EXTREME
Generation Outages During Extreme Cold Weather	HIGH
Nation-State Threats	HIGH
Supply Chain Compromise	HIGH
Malicious Insider Threat	HIGH
Inadequate Inverter-Based Resource and Distributed Energy Resource Performance and Modeling	HIGH

Additional details on these top risks and key takeaways are included in this report.



Summary of Top Regional Risks

Uncertain Energy Availability

Early retirement of thermal resources (e.g., coal and nuclear) that provide on-demand, dispatchable electricity generation creates potential energy shortfalls when replaced with variable, weather-dependent resources that may not be available when needed. This risk is amplified by increasing electricity demand (driven by electrification and the addition of large, single-point loads like data centers) and extreme weather. New approaches to assessing resource adequacy must consider the evolution of energy supply and demand to improve bulk power system planning, operation and investment decisions. Furthermore, the retirement of thermal generation must be carefully managed until adequate replacement energy is available to meet anticipated demand.

Generation Outages During Extreme Cold Weather

More frequent and longer lasting extreme cold weather systems are creating broader challenges for electricity and natural gas supply. Electric generators have experienced much higher incremental and unexpected outages during extreme cold temperatures due to equipment freezing and inadequate natural gas fuel supply. NERC Reliability Standard EOP-012-2 (effective October 1, 2024) helps to mitigate extreme cold weather challenges by ensuring generator owners have developed and implemented extreme cold weather operation plans. Greater cooperation is also taking place between the electric and natural gas industries, in part due to the Gas-Electric Harmonization Forum led by the North American Energy Standards Board (NAESB). However, work remains to be done to implement the recommendations from the NAESB [forum report](#) published in July 2023.

Nation-State Threat

Nation-state threats from China, Russia, and Iran are well funded, sophisticated, and capable of targeting North American critical infrastructure to achieve strategic and political objectives. By gaining access to and exploiting native tools within critical infrastructure operating systems, these threat actors can evade detection and strike through a variety of methods at a time when maximum damage would be inflicted. Utilities need to enhance detection methods on critical operational control systems and develop business continuity plans to respond to and recover from various attack scenarios that could be conducted by a nation-state-sponsored threat actor.

Supply Chain Compromise

Malicious manipulation of a single vendor's hardware, software, services, or delivery could impact multiple utilities that use the vendor's products and disrupt grid operations. The limited number of industrial control system vendors that are used to protect and control the bulk power system creates a broad threat to grid reliability. Understanding the inherent risk of using third-party products, utilities should require vendors to improve their respective controls and operating environments. This includes vetting vendors for foreign connections with known hostile nations.

Malicious Insider Threat

Malicious insiders are considered to be an employee or a contractor/vendor integrated into the workplace that have motivation, knowledge, and legitimate access to launch an attack on a utility's systems or assets. An insider motivated by unmanaged workplace disgruntlement, ideological reasons, or financial gain can have the opportunity to compromise systems and render the systems inoperable which can degrade grid reliability. Utilities should have a robust Insider Threat Program supported by executive management that builds a culture of security and encourages employees to look out for each other and address potential insider attack if employees notice unusual behavior.



Utilities should also limit access to critical systems and assets to employees that have a business reason for access and segment systems to minimize impact. Utilities should also have processes and procedures to vet employees before granting access to critical assets.

Inadequate Inverter-Based Resource and Distributed Energy Resource Performance and Modeling

Inverters are used to connect wind, solar, and battery generation to the bulk power system and are predominately used to connect Distributed Energy Resources to distribution grids. Inverter-Based Resources (IBR) are a growing proportion of the electric generation fleet, which increases the grid's dependence on them to provide reliable energy. Unlike the physical response of conventional, thermal generation (e.g., coal and natural gas) resources, IBRs use configured controls to manage adverse grid conditions. Incorrect modeling of IBRs and the behavior of configured controls during grid disturbances has resulted in unexpected power losses, posing considerable risk to bulk power system reliability. Furthermore, the risk IBRs pose to reliability has not been properly considered in the planning of future grid investments. Utilities need to proactively mitigate IBR performance issues by closely monitoring grid conditions and collaborating with IBR owners and operators to set controls that ensure reliable operation.

Summary

MRO is uniquely positioned to coordinate and collaborate with various industry stakeholders to address the risks highlighted in this report. As a trusted authority on grid reliability and security, we are committed to raising awareness, providing guidance, and developing mitigation strategies for the highest risks to the regional bulk power system. Collaboration among multiple stakeholders is crucial to navigate the rapid changes and confront the many challenges facing the electricity industry, advancing our collective vision of a highly reliable and secure North American bulk power system.



3. INTRODUCTION

The purpose of MRO's Regional Risk Assessment (RRA) is to communicate the highest risks to reliability and security within the region so that utilities can prioritize activities to mitigate risk. The report is provided to industry stakeholders and policymakers to help inform decisions that impact grid reliability and security. The report highlights work that MRO and the broader ERO Enterprise (collectively NERC and the six Regional Entities, including MRO) is doing to track, trend, and mitigate each risk, including high-level action items and recommendations.

Industry Coordination and Collaboration

The RRA is developed by MRO staff in collaboration with industry experts from three subject matter specific advisory councils: Compliance Monitoring and Enforcement Program (CMEP), Reliability, and Security. These councils provide valuable input throughout the RRA development process by providing an industry perspective. In 2024, MRO conducted a stakeholder survey to gather additional industry perspectives on the identified risk themes. The findings of this survey and feedback from the advisory councils are incorporated into the RRA.

Inputs to the RRA Process

The RRA identifies and prioritizes risks based on several sources, including:

- Bulk power system disturbance and event reports (from the ERO Enterprise Event Analysis Program and EOP-004 reports filed with NERC by utility companies).
- MRO's Regional Security Risk Assessment (facilitated by the Security Advisory Council), Summer Reliability Assessment, and Winter Reliability Assessment.
- NERC continent-wide assessments, including the State of Reliability Report, Long-term Reliability Assessment, seasonal assessments, and the results of the Interregional Transfer Capability Study.
- NERC alerts to industry, published lessons learned, and other reliability guidelines.
- Generation and transmission availability data provided by industry.
- Industry transmission system misoperation data and related reports.
- Analysis by MRO's Compliance Monitoring Enforcement Program Advisory Council (CMEPAC) on the effectiveness of NERC Reliability Standards in addressing regional risks.
- Information gathered through MRO's Security Advisory Council Threat Forum (SACTF) - a stakeholder group that meets weekly to discuss regional security threats to bulk power system reliability.

NERC's [2023 ERO Reliability Risk Priorities Report](#) serves as the foundation for MRO's analysis, providing risk profiles and themes identified by industry stakeholders across North America. MRO adapts these North American-wide risk profiles and themes so that they are specific and relevant to the MRO region. The relationship between these regional risks and the North American risk profiles and themes is further detailed in Section 4 of this report.



About the MRO Stakeholder Survey

The stakeholder survey conducted in 2024 provided valuable insights into stakeholder needs, perceptions, and the significant trends, challenges, and opportunities facing industry. Participants included industry technical staff with operations or security expertise, executive and c-suite leaders, and state and provincial regulators. Figure 2 shows the mean scores to questions in the survey asking respondents whether they see each risk as a significant threat to the bulk power system. Respondents entered their scores on a scale of 1-6 with 1 indicating “strongly disagree” and 6 indicating “strongly agree”.

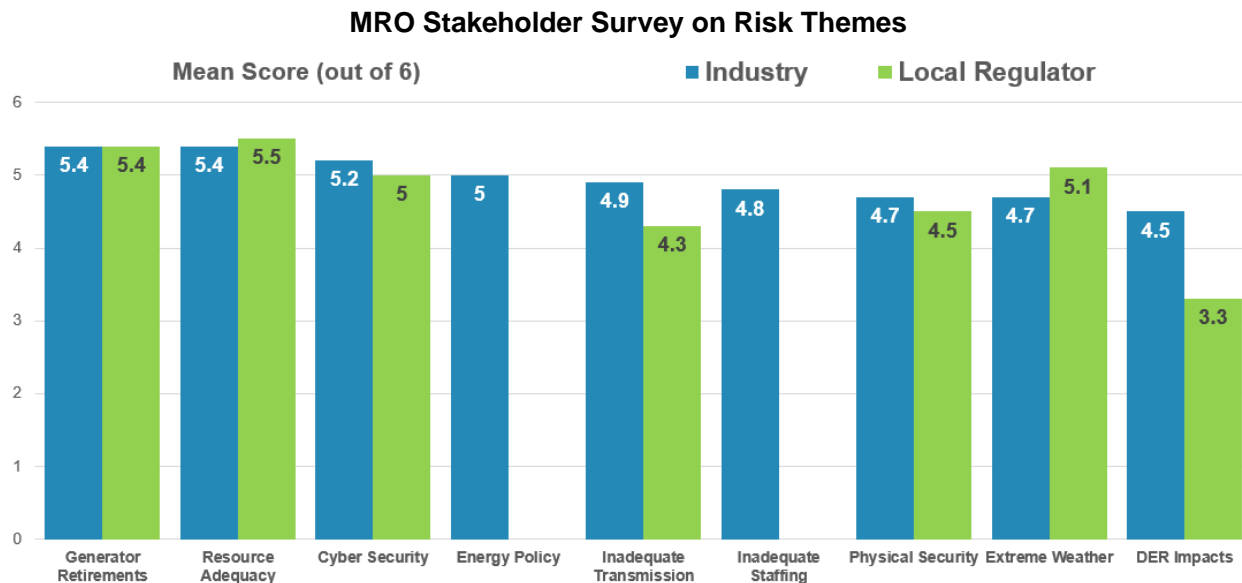


FIGURE 2 - RISK PERCEPTION SCORES FROM 2024 MRO STAKEHOLDER SURVEY

The results highlighted a shared concern among both industry and local regulators regarding the reliability impacts of the grid transformation, specifically the increasing reliance on variable, weather-dependent resources as traditional, dispatchable generation retires. Another key concern was ensuring adequate electricity supply to reliably meet demand across all times of day, seasons, and weather conditions. Cybersecurity threats were also identified as a major risk to the bulk power system. Concerns stemming from government policies, regulations, and inadequate transmission infrastructure were identified by industry respondents. These findings align with the top reliability and security risks identified in the RRA.

Actions to Reduce Risks

Much of MRO’s work in 2025 will be dedicated to reducing the extreme and high priority risks identified in this report. MRO will conduct outreach to raise awareness of the risks across the region and share actions that can be taken by industry to reduce risks, including improvements or additions of controls related to the prioritized risks.



Regional Risk Ranking Process

Figure 3 presents the current [Reliability Risk Matrix](#) used to prioritize the risks identified in the 2025 RRA.

The relative rank of each risk (location on the matrix) is the result of assessing the likelihood and impact of the risk on the regional bulk power system.

Impact is determined by how widespread a particular event or risk would be on the bulk power system. It considers a typical event for each risk instead of focusing on worst-case scenarios, which might elevate the risk to a higher impact.

Likelihood is assessed by evaluating three criteria:

- Mandatory Controls - Is a NERC standard in place to effectively mitigate the risk?
- Emerging Trends - Are the occurrences increasing?
- Event History - Are there any documented occurrences of the risk?

Risks are categorized into four levels: *Low*, *Medium*, *High*, or *Extreme* based on the risk impact and likelihood scores. Risks classified as High or Extreme are considered the most significant threats to reliability and security within the MRO region.

To determine the impact and likelihood of each risk, MRO staff collaborated with industry experts from the advisory councils. This involved a comprehensive review and discussion on each risk, followed by individual rankings from each expert. The collective scores for each risk were then averaged to determine its relative ranking on the MRO Reliability Risk Matrix.



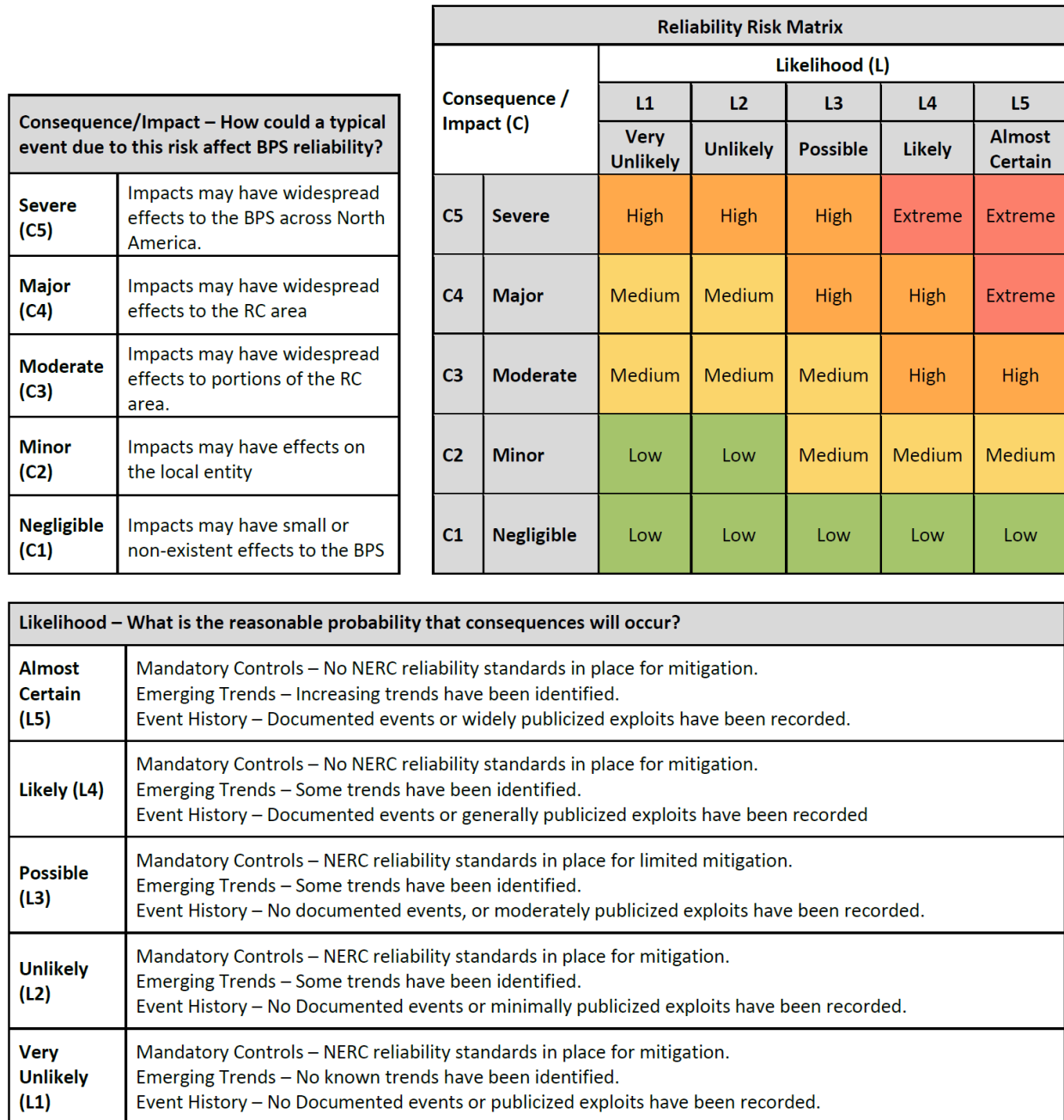


FIGURE 3 - MRO RELIABILITY RISK MATRIX



4. 2025 MRO REGIONAL RISKS AND RANKINGS

The following section summarizes the regional risks included in the 2025 Regional Risk Assessment. Table 2 and Figure 4 list the risks in the 2025 RRA and show the relative ranking of each risk.

Table 2: List of MRO Reliability Risks in the 2025 MRO RRA

Reliability Risks	
1 Uncertain Energy Availability	7 Phishing / Malware / Ransomware
2 Generation Outages During Extreme Cold Weather	8 Loss of Essential Reliability Services
3 Nation-State Threats	9 Physical Attacks
4 Supply Chain Compromise	10 Material and Equipment Availability
5 Malicious Insider Threat	11 Internet-Connected Devices
6 Inadequate Inverter-Based Resource (IBR) and Distributed Energy Resource (DER) Performance and Modeling	12 Use of Inaccurate Transmission Facility Ratings
	13 Tight Supply of Expert Labor
	14 Vulnerabilities of Unpatched Systems

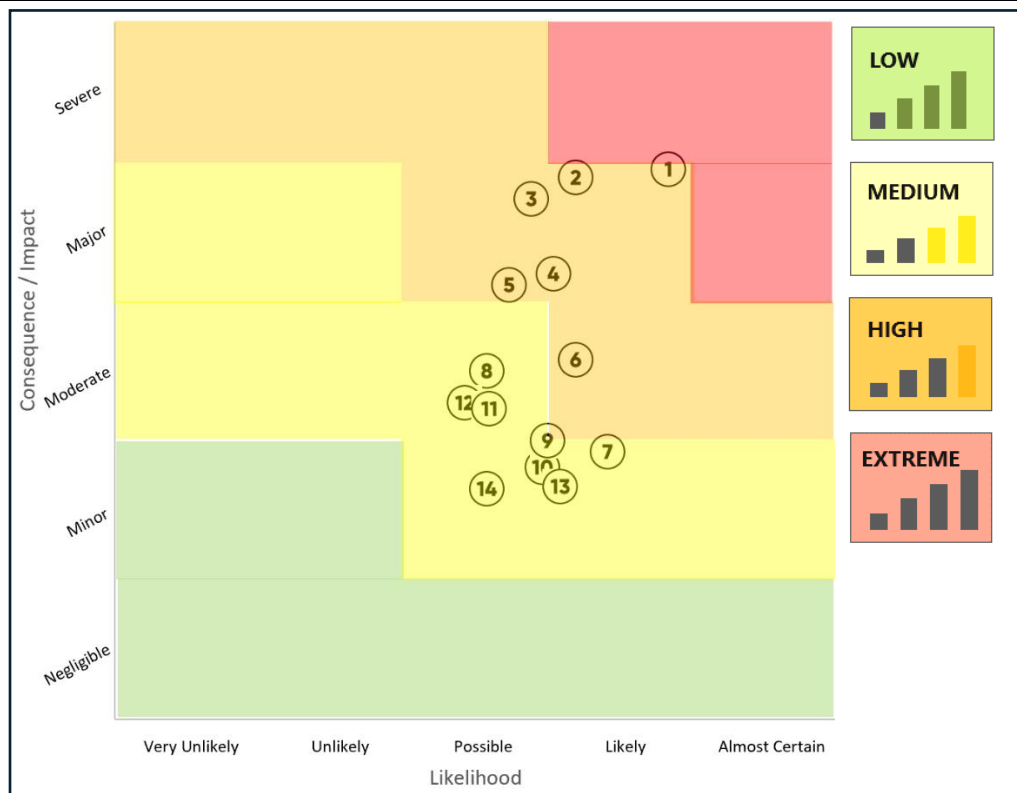


FIGURE 4 - RANKED MRO RELIABILITY RISKS HEAT MAP



The risk of *Uncertain Energy Availability* has been categorized as extreme for the second year in a row. The anticipated addition of large loads like data centers and industrial facilities will strain the current system to meet the energy demand these loads require. This risk is amplified by continued increases in variable, weather-dependent generation (i.e., wind and solar), which is difficult to forecast, and the load variability associated with new end uses of electricity (i.e., electric vehicles and home heating). All of this adds complexity to planning and operating the grid to meet electricity demand when it is needed.

In 2025, a significant new risk emerged: *Nation-State Threats* against electric infrastructure in pursuit of a nation's strategic objectives. Threat actors sponsored by nation-states such as China, Russia, and Iran aim to weaken a target nation's ability to respond economically or militarily during a conflict. To achieve this, they employ sophisticated and covert techniques to infiltrate and maintain a persistent presence within the target nation's systems. These actors use techniques to lie in wait, biding their time to strike at the most opportune moment.

The remaining four high risks identified on the heat map are listed below in order of highest to lowest priority:

- Generation Outages During Extreme Cold Weather
- Supply Chain Compromise
- Malicious Insider Threat
- Inadequate IBR and DER Performance and Modeling

Risk Prioritization Changes

The following three high category risks from the 2024 Regional Risk Assessment were downgraded to a medium priority in 2025, as shown in Figure 5.

- Loss of Essential Reliability Services
- Physical Attacks
- Material and Equipment Availability



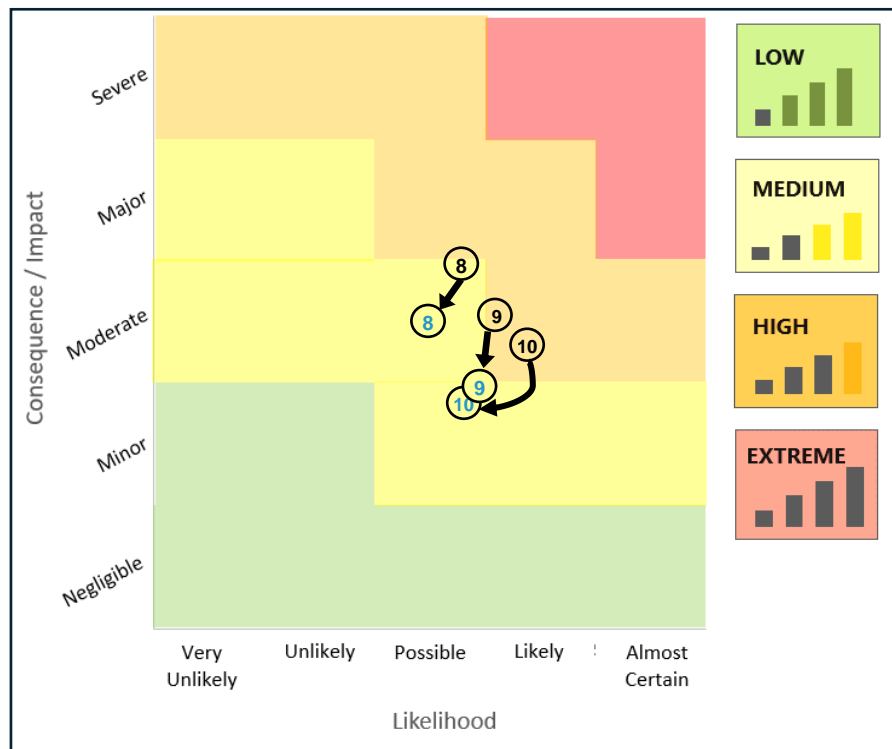


FIGURE 5 - HIGH PRIORITY RISKS THAT CHANGED IMPACT OR LIKELIHOOD CATEGORIZATION IN 2025

Risk No. 8 – Loss of Essential Reliability Services

The likelihood of this risk was reduced in this year’s assessment because there has not been a documented occurrence of a loss of essential reliability services resulting in a widespread system event. Additionally, mandatory NERC balancing reliability standards help to reduce this risk from a high to moderate level.

Risk No. 9 – Physical Attacks

This risk was heightened after the attacks on substations in Moore County, North Carolina in 2022. However, because there is limited potential for a physical attack to affect widespread portions of the region, the impact score of this risk was reduced from high to moderate. The likelihood of a physical attack to electrical infrastructure, however, continues.

Risk No. 10 – Material and Equipment Availability

Although lead times for critical electrical equipment have stabilized, this remains a challenge for utility companies across the region and has driven changes in how companies plan for grid repairs and expansion. Both the impact and likelihood of this risk were reduced because of the adjustments utilities have made to account for long lead times. The risk is, however, more impactful to smaller utilities that have fewer projects and resources to reduce the risk of equipment unavailability.



Dormant Risks

The following risks, previously identified as medium priorities, have now been effectively mitigated and/or are no longer considered significant concerns.

Misoperations Due to Human Errors

Misoperations on the bulk power system resulting from human error continue to decline, and the vast majority of these misoperations have had a negligible impact on overall system operations. Even the worst misoperations resulted in limited facility outages and minimal customer load loss. Utility companies across the region have been focused on reviewing system events and the human performance techniques associated with misoperations, which is expected to reduce the number of events even further.

Insufficient Physical Access Controls

This risk was primarily focused on threats of theft and vandalism to electrical infrastructure, and while the number of these events is on the rise, the vast majority do not impact bulk power system operations.

Correlation of ERO-wide risks and MRO Regional Risks

The [2023 ERO Reliability Risk Priorities Report \(RISC Report\)](#) identifies five evolving risk profiles to North American bulk power system reliability. These risk profiles form the framework for MRO's Regional Risk Assessment and regional risks are categorized within the risk profiles accordingly.



Energy policies at the federal, state, and local level impact how the bulk power system is planned and operated and have implications on system reliability. Policies decarbonizing electric generation threaten premature retirement of needed dispatchable resources to meet growing electricity demand and underlie the **Uncertain Energy Availability** risk in this report. At the same time, policies to electrify more parts of the economy, namely transportation and space heating, will change patterns in demand adding to forecasting complexity. State utility commissions and provincial regulators in MRO's region make generation and transmission investment decisions for consumers in their states. The **Loss of Essential Reliability Services** risk in this report identifies challenges for the future grid to provide adequate levels of the ramping, balancing, frequency response, and voltage support services. Support for investments that bolster these services are needed at the state and local levels because they have traditionally been difficult to quantify within energy markets. Policies to increase use of flexible loads and generation connected to the distribution system will increase the usage of **Internet-Connected Devices** to monitor and control supply and demand. This increases the cyber attack surface on systems that support bulk power system reliability that are outside the realm of enforceable NERC Reliability Standards.



Grid Transformation



The grid is transforming at a pace that has not been seen since the early twentieth century. The changing mix of resources away from dispatchable, on-demand generation to variable, distributed generation is having dynamic effects on the broader energy risk landscape. Variability in weather dependent energy resources is highlighted in the **Uncertain Energy Availability** risk in this report, which amplifies the need for new approaches to assessing energy adequacy (or ensuring energy is available when it is needed). As generation becomes more distributed across the bulk power system, essential reliability services (like voltage control and ramping) need to be planned for and available from different sources across the region's geographical footprint as outlined in the **Loss of Essential Reliability Services** risk in this report. The dynamic and configurable response of Inverter-Based Resources (IBR) depart from the physical response of synchronous machines, creating challenges with IBR performance and how these resources are modeled as described in the **Inadequate IBR and DER Performance and Modeling** risk in this report. As new technologies like IBRs are integrated onto the grid, there is limited expertise and resources to prepare for and resolve associated challenges as highlighted in the **Tight Supply of Expert Labor** risk in this report.

Resilience/ Extreme Events



Extreme weather systems are becoming more frequent, more severe, have broader impacts, and last longer than previously experienced. The impacts of these systems to the bulk power system have also increased, especially during extreme cold temperatures. The **Generation Outages During Extreme Cold Weather** risk in this report shows there is a significant increase in unexpected failures of electric generation caused by extreme cold temperatures. Additionally, the natural gas infrastructure that is relied upon by gas-fired electric generation has also been challenged during extreme cold weather. Resilience to extreme weather events is more difficult for storm-damaged facilities due to the supply chain challenges described in the **Material and Equipment Availability** risk in this report.

Security Risks



Critical infrastructure sectors, including the energy sector, are subject to a multitude of security threats. Threats posed by terrorists, criminal organizations, and **Nation-States** use increasingly sophisticated attacks seeking to undermine the confidence people have in the reliability of the bulk power system. **Physical Attacks** against transmission lines, substations, and generating plants create localized disruption of the system and customers. Use of third-party software and hardware creates **Supply Chain Compromise** risks where a threat actor can impact a significant portion of the grid by infiltrating the supply chain used by a large number of utilities. A **Malicious Insider Threat** with unique knowledge and access can strike physical or cyber targets within utility operations to inflict maximum impact to the bulk power system. **Phishing** is a well-known tactic to gain a foothold within systems to deploy **Malware** or **Ransomware** to either corporate or critical



control systems that could lead to an operational impact on the bulk power system. The **Vulnerabilities of Unpatched Systems** also provide a gateway into systems that are critical for the reliable operation of the bulk power system.

Critical Infrastructure Interdependencies



The bulk power system is dependent on many different infrastructure sectors (e.g., natural gas, communications, and water) for reliable operation. These industries also rely upon electricity for their operations, which creates a critical interdependency. This is particularly true for the **Generation Outages During Extreme Cold Weather** risk in this report, where the loss of natural gas supply during extreme cold temperatures has driven a large number of unexpected outages of natural gas-fired generation. As electric generation shortages due to lack of fuel persist during extreme cold, electric outages may occur and impact natural gas production, processing, and transportation infrastructure which would further limit gas supply.



5. DETAILED RISK INFORMATION

This section provides a detailed summary of each of the risks identified in the 2025 RRA in priority order starting with the extreme risk. Each summary includes information on the elements of the MRO Reliability Risk Matrix that were used in determining risk priority. Each element is briefly described below.

Key Drivers are the underlying factors or conditions that significantly influence the impact or likelihood of a risk. Key drivers can directly (within the industry's control) or indirectly (outside of the industry's control) influence the risk rating.

Emerging Trends are quantitative and qualitative metrics that reflect changes to the key drivers. Increasing trends result in a higher risk likelihood than trends that are more stable or not identified.

Event History encompasses past occurrences within the power system that are relevant to a specific risk. These events can stem from various aspects of bulk power system operations, planning, and physical or cyber security. Events that occur in other critical infrastructure sectors that have a high likelihood of occurring in the energy sector are also considered. Risks with frequent or extensive event histories are considered to have a higher probability of recurrence.

Mandatory Controls like enforceable NERC Reliability Standards are efforts in place to effectively mitigate risk. MRO's Compliance Monitoring and Enforcement Program Advisory Council (CMEPAC) conducts an annual analysis of the effectiveness of NERC Reliability Standards to reduce the risks identified in the RRA. Standards are rated on a scale from no control, low effective control, moderately effective control, and highly effective control. Risks that have moderately to highly effective controls are less likely to occur than risks with no mandatory controls or low effective controls. Where risks are currently being addressed through the development of new NERC Reliability Standards, this information is provided for context but not factored into the likelihood assessment of the risk.

Scenarios are examples of risk situations that could have significant impact on the bulk power system. Consistent with the MRO Reliability Risk Matrix, scenarios used are reasonable events with a range of outcomes that could occur if a risk is not mitigated. These scenarios are the basis for judging the impact of a risk.

Actions to Reduce Risk are recommendations for those responsible for the operations, planning, and physical and cyber security of the bulk power system to lessen the risk impact or likelihood. Where applicable, recommendations are provided for decision makers or other stakeholders who, while not directly controlling the system, can influence factors that directly or indirectly contribute to the risk.



Uncertain Energy Availability



Impact: Severe

Likelihood: Likely

A reliable bulk power system requires system operators to always maintain a constant balance between electricity supply and demand. Ensuring resources are available to maintain this balance is referred to as resource adequacy. Resource adequacy is accomplished by planning generation capacity around peak demand forecasts and including a reserve margin to account for random uncertainties, like unexpected generation outages (i.e., due to failure) or inaccurate load forecasts. Until recently, this method was effective because electricity supply was largely comprised of dispatchable plants that run on-demand with ample on-site storage of fuel. Electricity use was also stable and predictable based on historical consumption patterns from temporal data (like season, time-of-day, day-of-week, etc.) and weather.

The electricity resource mix, and how we use electricity, has evolved significantly over the past decade, rendering the traditional method for assuring resource adequacy insufficient on its own. As the generation fleet transitions away from dispatchable resources (like coal and nuclear) that are available on demand, to variable resources (like wind and solar) that are weather-dependent and cannot store fuel, there is greater risk of not having enough electricity available when needed. This is especially true during certain weather conditions when the fuel supply is constrained. At the same time, demand for electricity is skyrocketing. Data centers that run the internet, cloud computing, and artificial intelligence require massive amounts of energy. The deployment of electric vehicles and electric space heating is also growing rapidly. There is very little temporal data available on these newer uses of electricity. These are just a few of the factors that make it extremely difficult to accurately forecast future energy demand.

Key Drivers

- Federal, provincial, and state energy policies, along with electric utility companies' own initiatives to decarbonize the generation fleet, have accelerated proposed retirements of dispatchable generation (particularly coal and natural gas).
- Replacement sources of energy are more variable (wind and solar) and produce less energy overall than retiring generation.
- Queues for interconnecting new generation in the MRO footprint are long and are a barrier to bringing additional generation supply online to meet expected future energy demand.
- Systems to store energy from variable resources are commercially limited to short durations (typically 2-4 hours) and are currently unable to address long duration energy shortages (multi-day).
- Increases in large, single points of load (like data centers and industrial developments) are outpacing new generation being added.
- Demand growth from electric vehicles and space heating is difficult to predict and introduces more variability in electricity usage, making it harder to forecast when energy demand will peak.
- Limitations in the ability to transfer bulk amounts of energy over the electric transmission system from where there is ample supply to where it is needed.



- The lack of consistent and clearly defined energy adequacy metrics makes it difficult to identify future periods where there may not be enough energy to meet demand.

Emerging Trends

- The 2024 NERC Long-term Reliability Assessment (LTRA) projects a net reduction of up to 25 GW of dispatchable generation over the next five years in portions of the MRO region.
- During that same time, there is a projected net increase of 16 GW, possibly more, of variable generation. (It is important to note however, there is not a one-to-one comparison between variable and dispatchable resource output – it takes many more variable resources to replace the energy lost from retiring dispatchable generation.)
- The 2024 LTRA identifies areas within the MRO region that are at high or elevated risk of resource shortfalls during normal peak and extreme conditions over the next decade.
- Midcontinent Independent System Operator (MISO) is at high risk of energy shortfalls during normal peak conditions because of generator retirements beginning as early as 2025.
- Manitoba Hydro is at elevated risk of shortfalls during low-hydro conditions beginning in 2028, should drought conditions persist.
- Saskatchewan Power is at an elevated risk of shortfall, starting in 2026, for extreme conditions during the fall and spring seasons when more generation is offline for maintenance.
- Southwest Power Pool (SPP) is at an elevated risk of shortfalls beginning in 2025 during extreme demand conditions when coupled with low wind generation and natural gas fuel supply issues.

Figure 6 shows the ten-year peak demand growth and compound annual growth rate (CAGR) trends since 1996. Demand growth and CAGR reflect exponential upward trends since 2022 with CAGR at levels that have not been seen since the early 2000's. Peak demand growth is also expected to be significantly higher than the projections made just a few years ago. Specifically, peak demand growth for the winter season from 2025 to 2034 is anticipated to be nearly 150 GW, which is triple what was projected for 2022 to 2031. In the past five years of projections, peak demand growth in the winter season is outpacing summer demand growth, indicating a shift to more energy usage during the winter period.



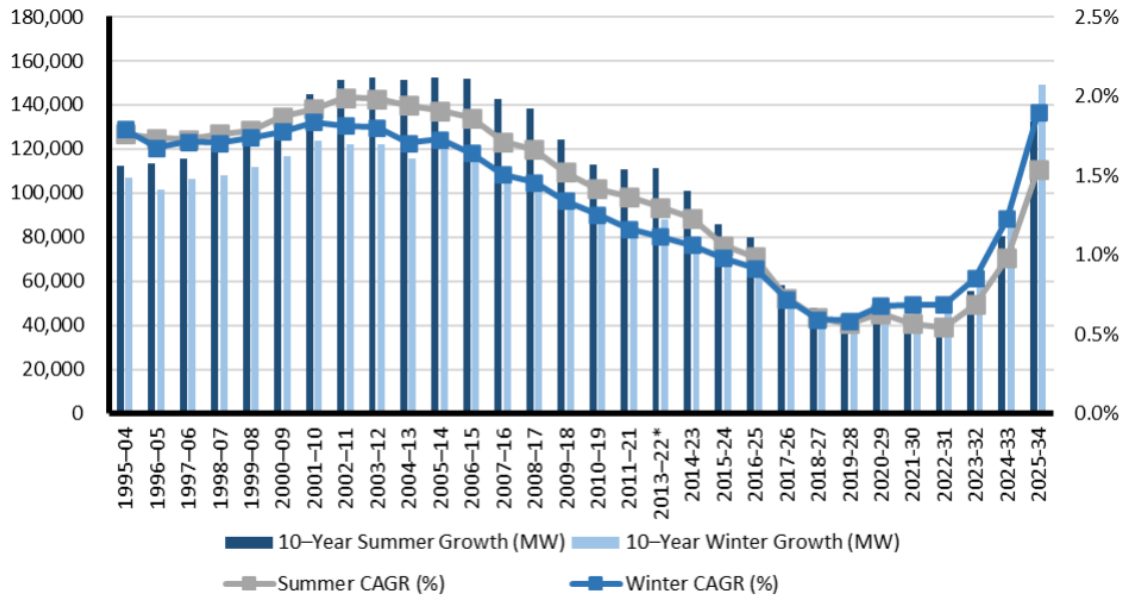


FIGURE 6 - 10-YEAR SUMMER AND WINTER PEAK DEMAND GROWTH AND RATE TRENDS¹

- According to the 2024 NERC State of Reliability Report, the Weighted Forced Outage Rate (WEFOR) in 2023 remained above the five-year average despite a lack of severe winter storms that elevated outage rates to all-time highs in 2021 and 2022. Forced outage rates of coal generation, in particular, have increased, attributed to reduced maintenance and abnormal cycling to accommodate variable resources.
- The ERO Enterprise Interregional Transfer Capability Study (ITCS) published in November 2024 shows the southern portion of the SPP footprint could benefit from an additional 3,700 MW of transfer capability by 2033 to resolve energy shortfall risks due to extreme weather.

Event History

- Winter storms Uri in February 2021 and Elliott in December 2022 brought abnormally low temperatures to portions of the MRO footprint and the broader United States. The extreme cold during both events caused unexpected generation outages that reduced electricity supply at the same time energy use was spiking. Around 5,400 MW of operator-initiated customer load shed was required to maintain system balance during winter storm Elliott. This is the largest amount of operator-initiated load shed in the history of the Eastern Interconnection. Over 23,000 MW of load shed was required, mostly in Texas, during winter storm Uri. This is the largest operator-initiated load shed in North America. Both events were due to a lack of available energy to meet demand.
- In a three-day stretch from January 23 to 25, 2024, wind generation output in the SPP and MISO Balancing Authority (BA) footprints produced a mere 6.5% of full nameplate capability. The minimum hourly wind generation output in that period was 1,222 MW out of over 58,000 MW of installed capacity. Electricity demand was successfully met within the two BAs using other resources and imported electricity from neighboring BAs.²

¹ From Figure 17 of the 2024 NERC [Long-term Reliability Assessment](#)

² Data derived from www.eia.gov [Hourly Electric Grid Monitor](#)



Mandatory Controls

There are no mandatory NERC Reliability Standards that explicitly require grid planners and operators to assess their ability to consistently meet electricity energy demand at all times. However, NERC is actively developing new standards to address this critical issue. The forthcoming standards will introduce the concept of energy reliability assessments that require grid planners and operators to assess their ability to meet demand across both short-term operations and long-term planning horizons. Below are links to the standards projects and their status.

[Project 2022-03 Energy Assurance with Energy-Constrained Resources](#) creates a new standard, BAL-007-1, requiring Balancing Authorities to assess the resources necessary to reliably supply energy to serve expected demand with operating reserves for a defined assessment period that is at minimum five days in duration and at maximum six weeks in duration. NERC's Board of Trustees approved the BAL-007-1 standard on December 10, 2024. The standard will become effective two years after FERC approval. At the earliest, it will be effective in 2027.

[Project 2024-02-Planning Energy Assurance](#) is intended to require industry to perform energy reliability assessments greater than one year out and determine actions to mitigate any energy deficiencies that are identified. A standard drafting team has been established for this project and work will soon begin to draft a new planning standard.

Scenarios

- The rapid decline of traditional power plants and their replacement with variable generation resources without an assured fuel supply continues, creating a supply-demand imbalance. This imbalance, coupled with sharp increases in electricity use, leads to significant energy shortfalls. If the shortages cannot be resolved with flexible demand reduction requests and/or through energy stored on the system, the grid operator will be forced to resort to load shedding, or intentionally cutting off power to certain customers to maintain the balance of supply and demand. Load shedding is a last resort to prevent a possible system collapse. The use of load shedding to address energy shortfalls, like those seen during winter storms Elliott and Uri, is increasing and could occur under less severe weather conditions.
- Two-day drought of wind and solar resource output, combined with planned maintenance outages of dispatchable generation, exceed energy storage capabilities and require load shedding to balance supply and demand for a multi-day period.
- A large number of utilities rely on energy imports to meet expected increases in electricity demand in their resource planning efforts. This leads to a broad under development of new generation across the region. A system event occurs with limited energy availability across the entire MRO footprint, reducing the availability of import capacity and requiring operator-initiated load shedding to maintain supply and demand balance.

Actions to Address Risk

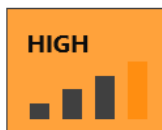
- The retirement of traditional, dispatchable power plants must be carefully managed to ensure a reliable and sufficient supply of electricity. In other words, there needs to be sufficient replacement energy available before these plants are phased out.
- Flexible, on-demand resources, currently provided by natural gas-fired generation, are crucial for addressing the intermittent nature of variable, weather dependent generation like



wind and solar. On-demand resources are capable of filling multi-day supply gaps when variable output is low and will be needed to meet anticipated increases in demand.

- Resource adequacy assessments should consider new metrics that go beyond the frequency-based criterion of the “Loss of Load Expectation” (LOLE), which determines resources needed to allow one-day of customer load loss in a ten-year period. Include supplemental criteria considering the size, timing, and duration of energy shortfalls. A co-sponsored NERC and National Academy of Engineers Section 6 report on [Evolving Planning Criteria for a Sustainable Power Grid](#) identifies the need for more robust metrics and criteria for resource adequacy. The report also highlights next steps to form an improved approach to resource adequacy.
- Improve load forecasting to comprehensively determine future load growth based on the likelihood and timing of deploying new end-uses of electricity, such as electric vehicles, electric space heating, and large, single-point loads like data centers and industrial facilities.

Generation Outages During Extreme Cold Weather



Impact: Major

Likelihood: Likely

Recent extreme winter weather storms Elliott in 2022, Uri in 2021, and to a lesser extent the artic storm from January 10-17, 2024 significantly challenged both the electric generation fleet and natural gas supply infrastructure to meet customer’s needs. Each of the storms resulted in higher than normal generation outage rates, which limited electric supply, and in the case of Elliott and Uri resulted in unprecedented calls to shed firm customer load to maintain the supply and demand balance and avoid significant system instability.

Key Drivers

- There is insufficient winterization of generation assets (particularly in the southern portion of the MRO footprint) to extreme cold temperatures, which includes inadequate freeze protection on thermal generation and cold weather cutouts of wind turbines.
- The production, processing, and transport of natural gas during extreme cold weather has had similar winterization issues, causing natural gas supply shortages.
- Natural gas infrastructure is more heavily relied upon during extreme cold weather to provide fuel “just in time” to an increasing number of gas-fired electric generators. At the same time, use of natural gas by consumers is increasing due to the extreme cold, resulting in natural gas shortages.
- The timing for utilities to procure the natural gas needed in the natural gas market does not always align with decisions to commit electric generation in the electric market, especially when commitments are needed with little lead time going into an operating day or during the weekend or holidays.
- The accelerated retirement of traditional, dispatchable power plants that can provide power on demand has reduced the available power supply. This reduced operating margin makes the system more vulnerable to significant energy losses when extreme cold weather causes power plant outages.



Emerging Trends

- Natural gas consumption reached a record high in January 2024 driven by gas usage during the arctic cold snap from January 10-17.³

Figure 7 from the [2023 NERC State of Reliability Report](#) shows the daily amount of generation lost due to unplanned outages in 2022. There were several winter storm events in 2022 that caused a spike in generator outages that were two to eight times the seasonal average. These outages during extreme cold weather are above the expected value shown by the red line.

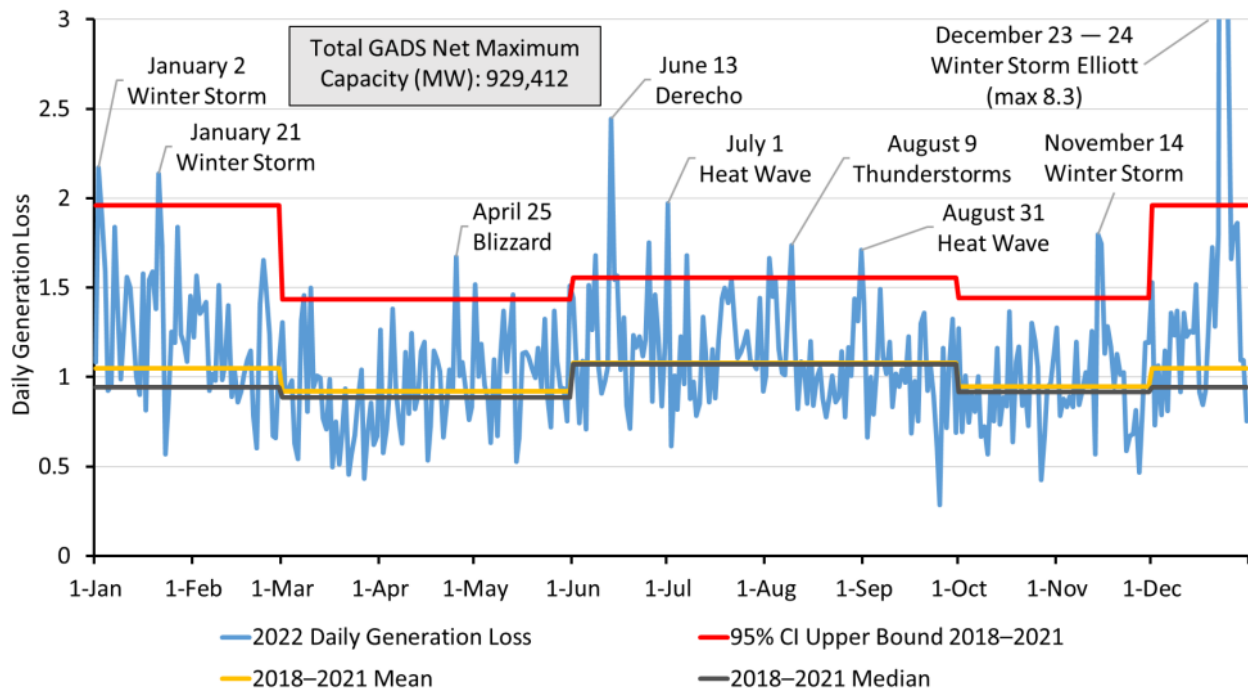


FIGURE 7 - 2022 DAILY GENERATION LOSS VS. SEASONAL AVERAGES

Event History

Five notable winter storms over the last decade have driven a large increase in unplanned outages of electric generation above the typical winter outage rate. Below is a list of these storms and the incremental, coincident amount of unplanned generation outages.

- Gerri and Heather (Jan 2024): unquantified amount of unplanned generation outages, but recognized as higher than typical winter outage rates.
- Elliott (Dec 2022): 90,500 MW
- Uri (Feb 2021): 61,300 MW
- Storm in South Central US (Jan 2018): 15,800 MW
- Storm in Central and Eastern US (Jan 2014): 19,500 MW

3

<https://www.eia.gov/pressroom/releases/press551.php#:~:text=The%20U.S.%20Energy%20Information%20Administration,led%20to%20high%20inventory%20withdrawals>



Mandatory Controls

NERC Reliability Standard EOP-012-2 (Extreme Cold Weather Preparedness and Operations) became effective October 1, 2024, requiring Generator Owners to calculate a minimum extreme cold weather temperature each of their generating units are capable of operating at. They do this by analyzing each generator unit's design, cold weather performance, and historical weather data to determine the lowest temperature the unit is likely to encounter. For units with an extreme cold weather temperature below 32 degrees Fahrenheit, Generator Owners must implement freeze protection measures to protect critical components. They must also develop and maintain comprehensive cold weather preparedness plans for each generating unit. Accountability for performance of the units at those temperatures is maintained by requiring corrective action plans for plants that do not operate as expected at the determined extreme cold weather threshold. While the standard is effective now, the requirement for the aforementioned items will not be enforceable until October 1, 2025. However, many Generator Operators have begun or completed work to comply with the standard's requirements because of several recent NERC Alerts issued related to winter weather preparedness.

Scenarios

- An extreme winter weather event like Elliott or Uri happens and is characterized by a blast of arctic air sweeping through the middle and eastern portions of the U.S., including the MRO footprint. During the storm, an extremely high rate of forced generator outages within the region occurs, requiring electricity imports from neighboring regions. Electricity imports are strained and eventually become unavailable due to broad, storm-related impacts to generation and transmission infrastructure in the neighboring regions. Subsequently, the shortfall in generation due to unplanned outages and limited imports requires load shedding to maintain the appropriate generation and load balance.

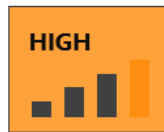
Actions to Reduce Risk

- Participate in MRO's [Generator Winterization Program](#), which assists utilities in preparing for extreme cold weather by assessing winterization methods and preparation specific to a generating plant and providing best practices and opportunities for improvement.
- Follow recommendations from NERC's Reliability Guideline on [Generating Unit Winter Weather Readiness](#) to prepare your generating plant for possible extreme cold weather conditions.
- Promote increased collaboration between the electric and gas industries to raise awareness of the interconnectedness of the two industries and protect reliability of both systems. If applicable to your organization, implement the recommendations identified by the North American Energy Standards Board report on the results of the Gas-Electric Harmonization Forum that occurred in 2023.⁴
- Consider the incremental increase of forced generation outages due to extreme cold weather in planning generation reserve margin requirements for an area.

⁴ https://www.naesb.org/pdf4/geh_final_report_072823.pdf



Nation-State Threats



Impact: Major

Likelihood: Possible

The strategic objectives of China, Russia, and Iran pose significant cyber threats to the United States. Their objectives vary but aim to weaken our military and economic capabilities. They are also interested in influencing foreign policy decisions. North Korea, while also a threat, is primarily motivated by financial gain. They are known for infiltrating IT organizations and focusing on cryptocurrency theft.

China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.

If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such a strike would be designed to deter U.S. military action by impeding U.S. decisionmaking, inducing societal panic, and interfering with the deployment of U.S. forces.

THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S
2024 ANNUAL THREAT ASSESSMENT

Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war. Moscow views cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets.

Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries.

THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE'S
2024 ANNUAL THREAT ASSESSMENT






“

North Korea’s cyber program will pose a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang’s cyber forces have matured and are fully capable of achieving a variety of strategic objectives against diverse targets, including a wider target set in the United States and South Korea.

North Korea will continue its ongoing cyber campaign, particularly cryptocurrency heists; seek a broad variety of approaches to launder and cash out stolen cryptocurrency; and maintain a program of IT workers serving abroad to earn additional funds.

”

THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE’S
2024 ANNUAL THREAT ASSESSMENT



“

Ahead of the U.S. election in 2024, Iran may attempt to conduct influence operations aimed at U.S. interests, including targeting U.S. elections, having demonstrated a willingness and capability to do so in the past. During the U.S. election cycle in 2020, Iranian cyber actors obtained or attempted to obtain U.S. voter information, sent threatening emails to voters, and disseminated disinformation about the election. The same Iranian actors have evolved their activities and developed a new set of techniques, combining cyber and influence capabilities, that Iran could deploy during the U.S. election cycle in 2024.

”

THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE’S
2024 ANNUAL THREAT ASSESSMENT

The Nation-State Threat focuses on threat actors that are well funded, capable, have effective cyber tools, and motivated to support their nation’s strategic objectives. They accomplish their goals by infiltrating targets, maintaining persistence, and waiting for the right time to strike. A nation-state threat is not motivated by quick financial gain like those captured in the Phishing/Ransomware/Malware and Physical Attack risks. These individuals or groups might target the bulk power system directly or use indirect methods, such as gaining access through IT systems to cause business continuity issues, gain access to lower voltage distribution systems, or affect supporting sectors. Additionally, a nation-state-sponsored threat actor may use any of the other risks

⁵ www.cisa.gov



in this RRA report as vector (note that there are events attributed to nation-states in both the *Supply Chain Compromise* and *Insider Threat* risks).

The Nation-State Threat underscores a set of techniques known as Living Off the Land, which leverage tools that already exist in bulk power system operating environments. In doing so, the threat actor remains stealthy and hard to detect because they defy conventional indicators of compromise associated with malicious activity. This is possible through built-in command line tools, other native tools and processes on the system, and absence of malware artifacts.

Key Drivers

- Heightened geopolitical tensions with China and challenges to the United States in its world economic and military influence.^{6,7}
- Heightened tensions with Russia over the continuing conflict in Ukraine, and strengthened ties with China, Iran, and North Korea.^{6,7}
- Organizations in the region are unprepared for this risk, still at the stage of scoping their response. Work is needed to develop and implement internal controls that detect, contain, and remove this threat.^{6,7}
- Living Off the Land is a set of techniques challenging even the most mature existing controls and detection.

Emerging Trends

- Nation-state threats are increasingly using digital and physical means to influence U.S. citizens by repressing dissent, manipulating public opinion, and weakening or undermining our capabilities to respond to global threats. This trend highlights the sophisticated methods and long-term strategies employed by these actors to achieve strategic objectives.⁷
- China is continuing to focus on critical infrastructure assets that provide little espionage or intelligence value, but collectively could enable disruption of military capability or disruption of health and human services.⁸

Event History

- China-sponsored Volt Typhoon threat actors gained access to U.S. and Indo-Pacific critical infrastructure sectors in 2023, including communications, energy, transportation, and water and wastewater systems. The Volt Typhoon group was pre-positioning itself on IT networks to enable lateral movement to OT assets to disrupt critical functions.⁸
- China-sponsored threat group BlackTech compromised routers in 2023. They used the compromised routers to expand their access via trusted network relationships to companies headquartered in the United States and Japan. BlackTech targeted government, telecommunications, and organizations that support the military, and used the compromised routers to deliver malware to victim operating systems.⁹
- Russia-sponsored Sandworm used Living Off the Land techniques in 2022 to execute a successful cyber attack against a Ukrainian electric utility, causing massive power outages.

⁶ [2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf](#)

⁷ [ATA-2024-Unclassified-Report.pdf](#)

⁸ [PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA](#)

⁹ [People's Republic of China-Linked Cyber Actors Hide in Router Firmware | CISA](#)



The cyber attack coincided with a series of missile attacks hitting Ukrainian critical infrastructure, some of which was already targeted by the cyber attack. Several days after the initial cyber attack, Sandworm also deployed malware to erase the contents of computers on the utility's network.^{10,11}

Mandatory Controls

- NERC Reliability Standards CIP-005-7 (Electronic Security Perimeter), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-007-6 (System Security Management), CIP-010-4 (Configuration Change Management and Vulnerability Assessments), and CIP-011-3 (Information Protection) provide defense in depth strategies to limit the movement of a threat actor within defined segments of a system, limiting access to defined repositories of power system information and system recovery. Collectively, these standards are controls protecting medium and high impact Bulk Electric System cyber equipment.
- NERC Reliability Standard CIP-007-6 (System Security Management) provides requirements for logging information at the host level that could be used to detect an adversary's activities.

On January 19, 2023, the [FERC issued Order 887](#) directing NERC to develop standard requirements for internal network security monitoring (INSM) for high and medium impact [Bulk Electric System Cyber Systems](#). NERC initiated a project to develop a new standard to comply with this order.

[Project 2023-03 Internal Network Security Monitoring \(INSM\)](#) creates a new standard, CIP-015-1, to provide Internal Network Security Monitoring for Bulk Electric System cyber equipment at high and medium impact assets. This improves the probability of detecting anomalous or unauthorized network activity by a malicious insider and improves response and recovery from an attack. This new standard was filed with FERC on June 24, 2024, and is awaiting approval.

Scenarios

- Nation-state adversaries are already on critical infrastructure company IT and OT assets. A nation-state conducts a cyber attack that physically destroys critical bulk power system operating equipment and causes widespread power outages. A coordinated attack on multiple generation assets and supporting sectors (like the natural gas system) occurs across the region, affecting a large portion of the North American bulk power system.
- A nation-state adversary is already on the IT and OT networks of North American Independent System Operators. They conduct a cyber-attack that corrupts control center to generator communications and sends erroneous setpoints to generators across the region. This causes multiple generators to trip offline and corrupts the digital back-ups of the affected Independent System Operator systems, which extends the restoration time. This scenario would affect a large portion of the Eastern Interconnection.

Actions to Reduce Risk

- Enhance detection on Operational Technology systems through data-analytics using existing logging, Internal Network Security Monitoring, and expanded endpoint activity logging.

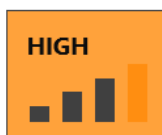
¹⁰ [Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike | WIRED](#)

¹¹ [Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology | Google Cloud Blog](#)



- Analyze controls to see where there is a lack of visibility to detect adversary activity.
- Bolster controls on data integrity and consider anomaly-based detection on control system values. (This is in addition to integrity controls while data is in transit, such as hashing.)
- Seek input from Operational Technology and Industrial Control System engineers, as these frontline workers often know system design vulnerabilities and can provide insights on where to monitor adversary activity.
- Develop business continuity plans for nation-state attack scenarios. Include plans to address a direct attack on infrastructure and an indirect attack on dependent infrastructure (GPS, operations-critical telecom, etc.). Plans for indirect attacks should focus on organizations that can continue to operate given the loss of support.

Supply Chain Compromise



Impact: Moderate to Major

Likelihood: Possible to Likely

A supply chain compromise occurs when a vendor is the vector for a security breach. It occurs because a threat actor manipulates hardware, software, connected services, or software delivery mechanisms. The manipulation occurs in a manner that the products or services that are purchased by utilities are already affected before they are integrated into a system. This risk also encompasses a vendor employee delivering a security compromise (e.g., implanting malicious code while servicing equipment).

The threat actor associated with this risk is likely more capable than the threat actor motivated by quick financial gain and opportunistic targets, mostly because the complexity and level of effort is high to use the supply chain as an attack vector. This threat can manifest at the vendor due to poor enterprise security programs or insecure code development practices. Factors that may change the vendor's exposure include changes of ownership that affect security controls, introducing changes in policy and process, changing geo-locations for manufacturing, changes in hosting or staffing, or, further consolidation of vendors putting more products under fewer corporate umbrellas.

Key Drivers

- There are complex and interconnected supply chains for the software and equipment deployed on the bulk power system and the inherited trust relationships that come from suppliers to those vendors.
- There is a growing reliance on common third-party providers across the industry.
- Security experts across the region participated in a Regional Security Risk Assessment that indicated there is a perception of high risk to control systems of bulk power system facilities in the region.
- Adversaries are increasingly taking advantage of supply chain complexity. Threat actors are capable because of the complexity required to execute an attack via a supply chain.





FIGURE 8 - INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN LIFECYCLE AND EXAMPLES OF THREATS¹²

Figure 8 represents aspects of the software supply chain and is used to illustrate that a vendor can be a vector of compromise at many stages of product and service lifecycle. Lack of security controls utilities put in place that are less effective the closer the lifecycle is to the vendor’s core processes exacerbates this risk. At these stages, controls rely on contractual agreements aimed at influencing vendor’s policy, process, and procedural safeguards. These are inherently less direct and harder to enforce.

Emerging Trends

- Inverter-based resources (IBRs) continue to expand and connect to the bulk power system at lower voltage distribution levels. The amount of new equipment and reliance on third party services for IBRs is increasing.
- More than 75 percent of software supply chains were exposed to cyber attacks in the last year.¹³

¹² CISA, NIST – Defending Against Software Supply Chain Attacks

¹³ [Software Supply Chain Attacks Have Increased Financial and Reputational Impacts on Companies Globally, New BlackBerry Research Reveals](#)



- Software supply chain incidents are increasing, with 43 percent of 1,650 security executives across 16 global industries, including utilities, experiencing issues within the last two years.¹⁴

Event History

- Red Hat, the maker of an enterprise Linux operating system, released an urgent alert in 2024 that a popular open-source Linux package (XZ Utils) was compromised. The individual responsible for maintaining the project on the open-source code development website injected malicious code. The code gave them unauthorized remote access to operating systems that included the package.¹⁵ The Linux operating system is widely used in utilities' operational control systems.
- Kaseya provides software for managed service providers (MSPs). In 2021, ransomware was deployed within Kaseya's software and infected the MSPs and their clients. About 1,000 companies were infected, impacting their ability to complete business functions. Over 140 MSPs were attacked.¹⁶ This is an example of how third-party relationships could affect many utilities and lead to operational issues.
- A failed update on CrowdStrike software in 2024 caused one of the largest IT outages in North American history. Windows computers critically failed and could not be rebooted.¹⁷ Although this incident has not been associated with a malicious actor, it is considered here because it illustrates the broad extent to which a software supply chain issue can affect our industry.

Mandatory Controls

- NERC Reliability Standard CIP-013-2 (Supply Chain Risk Management) provides moderately effective controls for most Bulk Electric System cyber equipment at medium and high impact assets. The standard requires that organizations develop and implement supply chain risk management plans. CIP-013-3, filed and pending regulatory approval, was modified to include virtualized cyber assets such as hosts and storage, which will bring more equipment into scope.
- NERC Reliability Standard CIP-005-7 (Electronic Security Perimeters) is applicable to Bulk Electric System cyber equipment at medium and high impact assets and has requirements designed to manage vendor remote access.
- NERC Reliability Standard CIP-003-9 (Security Management Controls), which is subject to future enforcement, is applicable to Bulk Electric System cyber equipment at low impact assets. It is less effective in mitigating supply chain risk because it only addresses supply chain risk through vendor remote access, which is not as expansive as the supply chain risk management requirements that are applicable to medium and high impact assets.

Scenarios

- A threat actor compromises control system vendors that serve bulk power system facilities with widespread implications, like the extent of the recent CrowdStrike incident where widespread adoption of a common IT vendor and platforms crashed Windows systems

¹⁴ [State of Security 2024: The Race to Harness AI | Splunk](#)

¹⁵ [Supply Chain Attack: Major Linux Distributions Impacted by XZ Utils Backdoor - SecurityWeek](#)

¹⁶ [Ransomware Attack Affecting Likely Thousands of Targets Drags On - WSJ](#)

¹⁷ [CrowdStrike outage explained: What caused it and what's next](#)



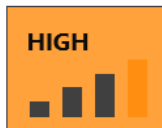
globally. In this case, compromised software directly controlling multiple utility systems has serious reliability consequences on large portions of the bulk power system. The industry simulated a similar scenario in 2024 where inter-control center data was interrupted due to a supply chain attack.

- A threat actor compromises a cloud-based generation management service and multiple low-impact wind or solar generation assets are affected. This causes a significant aggregate impact to the bulk power system.

Actions to Reduce Risk

- Understand the inherent risk of third parties. For example, determine how the vendor's cyber systems are segmented and what the largest impact to your operations would be if that cyber system was rendered inoperable.
- Contractually require vendors to make process and procedure changes to improve controls and reduce third-party risk.
- Support changing equipment specifications and systems architecture so operational control systems that operate the bulk power system are more resilient to attack.
- Vet vendors for foreign involvement with hostile nations. Security and Exchange Commission filings show changes in control, changes in management, major acquisitions, and company financial health.
- Review [NERC-filed comments on FERC Notice of Potential Rule Making RM-24-4-000](#). In the filing, NERC supports the proposed directives to address identification of, assessment of, and response to, supply chain risk, and expanding coverage to an additional type of Bulk Electric System cyber equipment.

Malicious Insider Threat



Impact: Major

Likelihood: Possible

The malicious insider is an employee, a contractor, or a vendor that is integrated into the workplace and has a certain level of access to company systems. These individuals possess motivation, insider knowledge, and the required permissions to launch a physical or cyber attack on a utility's general corporate network, operational control systems of the bulk power system, and/or physical assets. An insider may be motivated by unmanaged workplace dissatisfaction, ideological beliefs, or financial gain. A malicious insider may not be acting alone - they might have been recruited and manipulated by an outsider. An insider can use their knowledge of, and access to, critical systems to compromise or render them inoperable. Legitimate access to the target system or asset allows an insider to escape detection while setting up and executing the attack.

This risk does not include unintentional insiders who lack motivation. For example, an employee that is the target of a successful phishing attack but does not show a pattern of willful harm would fall under the Phishing/Ransomware/Malware risk.



Key Drivers

- There are limited detective controls during the precursory stages of an attack. Technical indicators, such as computer logging of suspicious events, typically occur after an insider has begun their attack.
- Through the Regional Security Risk Assessment, security experts within the MRO region classified this risk as high because of the access a malicious insider might have to control systems that operate the bulk power system.

Emerging Trends

- There are many examples of financially motivated insider threats across other sectors and government.
- Continuing social and political unrest provides ideological motivation.
- Utilities are increasing the use of contracted services, which may not be subject to the same controls as direct employees.

Event History

- Between January 30 and February 1, 2024, an employee at a Canadian nuclear plant in Ontario made online posts about security vulnerabilities at the plant. The employee was charged under Canadian law that prohibits communicating “safeguard information” to a foreign entity or terrorist group.¹⁸
- An infrastructure engineer at an industrial company locked systems, deleted backups, and changed passwords to extort the company for a \$750,000 ransom to restore access.¹⁹ This event is provided to highlight the type of impact workers could have on systems used to control bulk power system assets.

Mandatory Controls

- NERC Reliability Standards CIP-005-7 (Electronic Security Perimeter), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-007-6 (System Security Management), CIP-010-4 (Configuration Change Management and Vulnerability Assessments), and CIP-011-3 (Information Protection) provide technical methods for defense in depth, limiting movement of a threat actor to certain segments of a system, limiting access to defined repositories of power system information, and system recovery. Collectively, these standards are controls protecting Bulk Electric System cyber equipment at medium and high impact assets. However, these standards do not cover low impact assets that could still affect system reliability.

On January 19, 2023, the [FERC issued Order 887](#) directing NERC to develop standard requirements for internal network security monitoring (INSM) for high and medium impact Bulk Electric System Cyber Systems. NERC initiated a project to develop a new standard to comply with this order.

¹⁸ [Former Ontario nuclear plant operator employee charged in secretive leak case | Globalnews.ca](#)

¹⁹ [Man attempted \\$750K extortion of former NJ employer, feds allege](#)



[Project 2023-03 Internal Network Security Monitoring \(INSM\)](#) creates a new standard, CIP-015-1, to provide Internal Network Security Monitoring for Bulk Electric System cyber equipment at high and medium impact assets. The coverage will improve the probability of detecting anomalous or unauthorized network activity by a malicious insider to facilitate improved response and recovery from an attack. This new standard was filed with FERC on June 24, 2024, and is awaiting FERC approval.

Scenarios

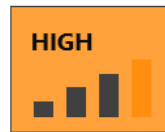
- A nonviolent but malicious insider intent on causing adverse impact to the bulk power system executes a cyber attack that affects a large portion of the grid in MRO's region, especially if the attack was targeted at a Balancing Authority or Reliability Coordinator. This would be a direct attack by a knowledgeable worker on operational control systems of the bulk power system at a company that has connections to power system assets of multiple utilities. The ability to impact facilities across a broad area increases the reliability impact from the attack.
- A nonviolent but malicious insider intent on causing adverse impact to the bulk power system executes a cyber attack on transmission or generation companies that affect power system assets of that utility. This would be a direct attack by a knowledgeable worker on operational control systems of the bulk power system.
- A violent and malicious insider physically attacks bulk power system facilities through kinetic means, such as guns, bombs, or vehicles with the intent to cause system outages. The impact of this risk is elevated over physical attacks by outsiders because the malicious insider has unique information and access that could increase the impact.
- A nonviolent malicious insider that targets the general corporate network of a utility executes a cyber attack that affects the power system assets of that utility. Since this is an indirect attack and the operational control systems of the bulk power system are not directly affected, the bulk power system would only be impacted if the utility does not recover from the incident.

Actions to Reduce Risk

- Collaborate with others across the company to develop an Insider Threat Program with support from top management. MRO has an Insider Threat Program Checklist that is available upon request to assist utilities with this effort.
- Build a culture of security within your organization through employee training, policies on the acceptable use of company resources, and reporting mechanisms for suspicious behavior. Concerned employees are the best early detector of insider threats.
- Offer employee support programs for mental health and wellness to reduce the risk of insider threats by managing dissatisfaction.
- Subject to applicable regulations, consider the use of behavioral analytics on employees' activities to help identify changes in work patterns and follow up on those changes.
- Move towards Zero Trust architecture, starting with operational control systems of the bulk power system. Verify each access request as if it originates from an untrusted network, as opposed to the perimeter method that assumes everything from within the trusted network is safe.
- Limit access to the least privilege for a job role. Limit the use of administrator accounts, review access grants, and monitor for access creep.
- Limit lateral movement by implementing more granular systems and network segmentation.



Inadequate IBR and DER Performance and Modeling



Impact: Moderate

Likelihood: Likely

Inverter-Based Resources (IBRs)—predominantly wind, solar, and battery—respond to grid conditions based on configured controls versus the physical response of large, rotating machines found in conventional generation. IBRs are relatively new technology for generating large amounts of electricity. As the utility industry and equipment manufacturers gain experience, they are still learning how to reliably integrate large numbers of IBRs into the power grid. Deployment of IBRs at customer sites, referred to as Distributed Energy Resources (DER), has grown and the number of these devices is less visible to system planners and operators. In aggregate, DERs can impact bulk power system operations. Whether at the high-voltage bulk power system or lower-voltage distribution level, incorrectly modeling the control behavior of IBRs can lead to planning assessments not properly accounting for the actual performance of these resources. Poor performance of IBRs can lead to unexpected losses of power from these resources that when aggregated together create unstable or insecure system operations.

Key Drivers

- IBRs are increasingly relied upon to serve energy needs as traditional power plants are retired.
- The fast, electronic response of IBRs is challenging to coordinate alongside the slower, physical response of traditional plants and other IBRs connected nearby.
- Even though individual interconnections of IBRs produce relatively smaller amounts of electricity than traditional power plants, the aggregate behavior of a group of IBRs can lead to large reliability impacts.
- IBRs are still early on the technology curve for grid-scale deployment. Industry engineers are only beginning to learn the behavior and reaction of IBRs to grid disturbances and what information to provide to IBR developers and equipment manufacturers to maintain system reliability.
- There are a limited number of power system models that consider IBRs and a limited amount of expertise with these models within the utility industry to deploy them accurately.
- IBR developers and manufacturers are less familiar with electric operations, creating a challenge for integrating grid-friendly responses to abnormal conditions.
- Inverter settings can easily be changed remotely, which change the behavior of IBRs without the grid operator's awareness.



Emerging Trends

Figure 9 shows the breakdown for the generation types within the active MISO and SPP generation interconnection queues. Ninety-five percent of MWs in the queues are solar, battery/storage, hybrid, and wind, which are largely IBR. The vast majority of future generation development is expected to be IBRs.

MISO and SPP Active Generation Interconnection Queue

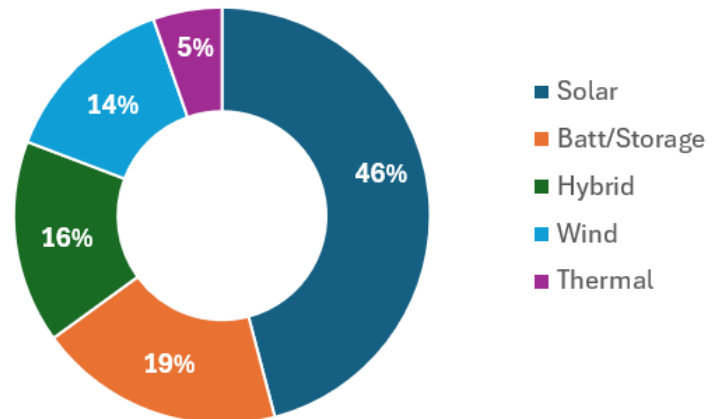


FIGURE 9 - PROPORTION OF GENERATION TYPES IN THE MISO AND SPP INTERCONNECTION QUEUES

- According to NERC's 2023 State of Reliability Report, the 2022 maximum contribution of wind and solar to meet total demand in MISO peaked at 39 percent and in SPP at 88 percent, indicating periods with heavy reliance on IBRs to serve load.²⁰

Event History

Since 2016, there have been 13 events involving the loss of IBR following a grid disturbance.²¹ The Blue Cut Fire disturbance²² was the first reported event in August 2016 and resulted in loss of 1,200 MW of IBR. NERC published actions and recommendations following this and subsequent events, yet additional events occurred over the next six years. In 2021 and 2022, there were two events near Odessa, Texas^{23,24} that resulted in a loss of 1,148 MWs and 1,711 MWs, respectively. Actions were taken by IBR owners after the first event to reduce the likelihood of recurrence, however, the second event resulted in a greater loss of MW output despite those actions.

Mandatory Controls

- NERC Reliability Standard TPL-001-5.1 (Transmission System Planning Performance Requirements) establishes transmission system planning requirements for the bulk power system to ensure reliable operation across a wide range of system conditions and potential system contingencies. The standard is minimally effective at reducing IBR risk because the technology is new, there is limited performance data, and current models are not required to incorporate DER performance.

²⁰ https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Technical_Assessment.pdf

²¹ https://www.nerc.com/pa/Documents/IBR_Quick_Reference_Guide_Activities.pdf

²² https://www.nerc.com/pa/rrm/ea/1200_MW_Fault_Induced_Solar_Photovoltaic_Resource_/1200_MW_Fault_Induced_Solar_Photovoltaic_Resource_Interruption_Final.pdf

²³ [https://www.nerc.com/comm/RSTC_Reliability_Guidelines/NERC_2022_Odessa_Disturbance_Report%20\(1\).pdf](https://www.nerc.com/comm/RSTC_Reliability_Guidelines/NERC_2022_Odessa_Disturbance_Report%20(1).pdf)

²⁴ https://www.nerc.com/pa/rrm/ea/Documents/Odessa_Disturbance_Report.pdf



- NERC Reliability Standard MOD-032-1 (Data for Power System Modeling and Analysis) establishes modeling data requirements to support analysis of bulk power system reliability. This standard does not recognize the uniqueness of IBR modeling for the same reasons mentioned above, which limits its effectiveness.
- NERC Reliability Standard PRC-024-3 (Frequency and Voltage Protection Settings) sets requirements for generating resources to remain connected to the system during disturbances. Because IBR performance requirements are not defined in this standard, it is very limited in reducing IBR risk. To address this limitation, NERC developed modifications to the standard as part of Project 2020-02, which is reviewed below.

On October 19, 2023, FERC issued [Order 901](#) directing NERC to modify or create new Reliability Standards that address IBR-related deficiencies in the standards. NERC established a three-phase work plan in early 2024. Phase one of that work plan resulted in several standard developments to address the inadequate performance and modeling of IBRs, which are detailed below. The remaining phases will be implemented in 2025 and 2026.

[Project 2020-02 Modifications to PRC-024](#) calls for a new standard, PRC-029-1, to supplement PRC-024 that specifies IBR requirements to remain connected to the system during disturbances. PRC-029-1 was approved by the NERC Board of Trustees on October 8, 2024, and filed with FERC on November 4, 2024. The implementation plan for this standard has elements going into effect as early as 2026 and 2027.

[Project 2021-04 Modifications to PRC-002](#) calls for a new standard, PRC-028-1, to supplement PRC-002 with specific requirements to provide adequate data to evaluate IBR performance during disturbances and to provide data to validate IBR models. PRC-028-1 was also approved by the NERC Board on October 8, 2024, and filed with FERC on November 4, 2024.

[Project 2023-02 Analysis and Mitigation of BES Inverter-Based Resource Performance Issues](#) calls for a new standard, PRC-030-1, to identify, analyze, and mitigate events similar to what has been experienced since 2016. It places accountability for the performance of IBR(s) on Generator Owners and increases awareness of the frequency and volume of issues experienced with IBRs on the bulk system, as well as steps taken to address these issues. The standard will become effective one year after approved by FERC.

Scenarios

The following scenarios assume a continued increase in wind, solar, and battery resources that lead to operating conditions where most of the energy is served by IBRs.

- A grid disturbance within the MRO region causes a large number of individual IBR interconnections to cease operation, resulting in a loss of real power that is larger than the greatest single generation contingency planned for the region. This leads to a reduction in grid frequency that, if severe enough, would require under-frequency load shedding to stabilize the frequency decline.
- An area of the MRO footprint with very high penetrations of IBRs and no traditional, synchronous generators leads to low fault currents and results in misoperations of protective relays. This leads to equipment damage and failure and results in customer power outages.

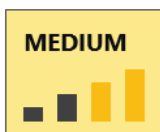


- A pocket of IBRs within the MRO footprint are not coordinating with each other, which leads to grid oscillations that interact with other grid devices and results in equipment damage and customer power outages.

Actions to Reduce Risk

- Proactively mitigate performance challenges with IBRs by monitoring their response following grid disturbances and collaborating with IBR owners and operators to correct incorrect responses. Openly share identified issues and solutions so others can learn from these experiences.
- Follow industry recommendations from a Level 2 NERC Alert on development and use of models for IBRs in wide-area studies and interconnection-specific analyses.²⁵
- Follow industry recommendations from a Level 2 NERC Alert to ensure inverter protection settings appropriately maximize availability of resources during and following a grid disturbance, while respecting inverter and substation equipment limitations.²⁶
- Seek information published by NERC's Inverter-Based Resource Performance Subcommittee, which was formed in 2021 to focus on the reliable integration of IBRs into the bulk power system. In addition to the standards updates provided in the Mandatory Controls section above, the subcommittee has published reliability guidelines, white papers, event analysis, webinars, and gap analysis for IBR challenges not addressed by the NERC standards. Specific topics include electromagnetic transient modeling and simulations, interconnection studies for IBRs, grid forming technology, battery energy storage and hybrid plants, and IBR and hybrid plant frequency response.²⁷
- NERC is implementing the FERC-approved work plan to identify and register bulk power system connected IBR owners and operators. This is a three-year project that started in May 2023 and is scheduled to be completed in May 2026. The purpose of this initiative is to address a reliability gap associated with bulk power system-connected IBR resources that are currently not registered with NERC or required to comply with NERC standards.

Phishing / Malware / Ransomware



Impact: Minor

Likelihood: Likely

This risk is a correlated grouping of three separate cyber threats. Phishing attacks trick employees into clicking on a malicious link or opening harmful files within the email. This compromises the utility's systems by introducing malware, or software designed to harm or exploit the victim's computer systems. Ransomware is a type of malware that encrypts the victim's files, rendering them inaccessible until a ransom is paid.

The threat actors that employ these techniques are less sophisticated and are motivated by quick financial gain. Unlike the threat actors described in the higher-ranked security risks of Nation-State

²⁵ <https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC%20Alert%20Level%20%20-%20Inverter-Based%20Resource%20Model%20Quality%20Deficiencies.pdf>

²⁶ <https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC%20Alert%20R-2023-03-14-01%20Level%20%20-%20Inverter-Based%20Resource%20Performance%20Issues.pdf>

²⁷ [Inverter-Based Resource Performance Subcommittee \(IRPS\)](#)



Threats, Supply Chain, and Malicious Insider Threat who are highly capable and motivated to harm the bulk power system, the actors described here target employees and systems on general corporate networks because they are more accessible. Bulk power system operational control systems are typically not the target because they are more isolated from external access and there are fewer employees that work directly on those systems. However, a successful attack on a general corporate network could still result in adverse impact to operations, loss of sensitive data, and reputational damage. Examples of this occur when systems that directly support the bulk power system are affected, such as voice communications, identity and access management functions, market functions, and engineering support. Additionally, operational data pertaining to the bulk power system is often archived on general corporate network locations.

Key Drivers

- Risk to the bulk power system is perceived as lower because operational control systems are typically isolated.
- The relative size of the utility industry makes it a smaller target for opportunistic and financially motivated threat actors.²⁸
- Most social engineering breaches occur through email, which is a widely used system that can affect many layers of an organization.²⁹

Emerging Trends

Forty-five percent of 1,650 security executives across sixteen global industries, including utilities, experienced a ransomware incident within the last two years.³⁰

Figure 10 shows that phishing is holding steady across all sectors as a top entrance for system breaches. This illustrates that this risk still warrants attention in 2025.³¹

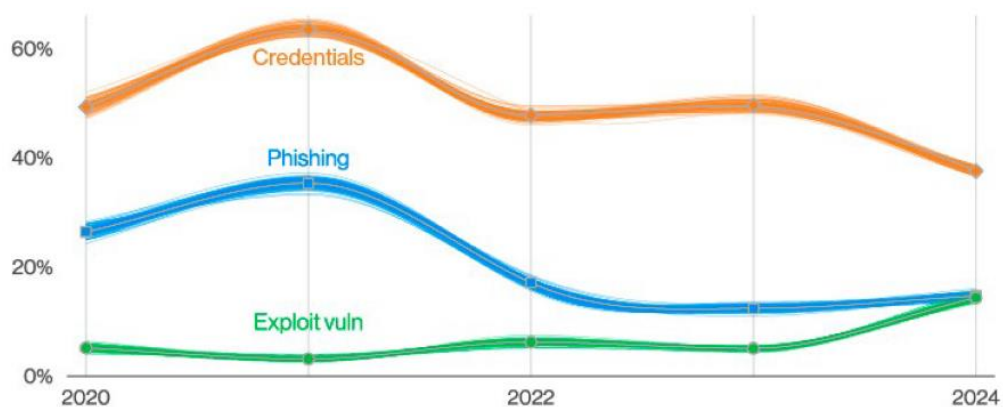


FIGURE 10 - TOP WAYS IN FOR NON-ERROR, NON-MISUSE BREACHES OVER TIME

²⁸ [Utilities saw fewer Q1 ransomware attacks than other sectors. A Dragos analyst explains why. | Utility Dive](#)

²⁹ [2024 Verizon Data Breach Incidents Report](#)

³⁰ [State of Security 2024 Report Reveals Growing Impact of Generative AI on Cybersecurity Landscape | Splunk](#)

³¹ [2024 Verizon Data Breach Incidents Report](#)



Event History

- Like most industries, there have been ransomware reports within the utility sector. In 2023 and 2024, sector companies compromised by ransomware attacks include but are not limited to Hitachi Energy³², Siemens Energy³³, Cognizant³³, Johnson Controls³⁴, ABB³⁵, and Schneider Electric³⁶.
- A ransomware attack on Colonial Pipeline corporate networks in 2021 resulted in significant disruption of the company's operations. The heavily used gas pipeline was shutdown to minimize the risk of exposure to the company's operational network.³⁷

Mandatory Controls

- NERC Reliability Standards CIP-005-7 (Electronic Security Perimeters), CIP-007-6 (System Security Management), and CIP-010-4 (Configuration Change Management and Vulnerability Assessments) are applicable to medium and high impact assets, and have requirements that are designed to segment operational cyber systems on networks that are associated with one facility, limit the penetration of malicious code and malicious communications through perimeter defenses, provide for system hardening, actively mitigate vulnerabilities, and provide software source and integrity verification. Although CIP-009-6 (Recovery Plans for BES Cyber Systems) does not specifically address the attack vector, it includes recovery requirements that support the continued functionality of the Bulk Electric System.
- NERC Reliability Standard CIP-004-7 (Personnel and Training) does not specifically reference phishing but has requirements for utilities to develop a security awareness and training program that periodically reinforces cyber security best practices. The human element is the first line of defense against phishing attacks, and well developed training programs are known to reduce successful phishing attempts.

On January 19, 2023, the [FERC issued Order 887](#) directing NERC to develop standard requirements for internal network security monitoring (INSM) for high and medium impact Bulk Electric System Cyber Systems. NERC initiated a project to develop a new standard to comply with this order.

[Project 2023-03 Internal Network Security Monitoring \(INSM\)](#) creates a new standard, CIP-015-1, to provide Internal Network Security Monitoring for Bulk Electric System cyber equipment at high and medium impact assets. The coverage will improve the probability of detecting anomalous or unauthorized network activity by a threat actor to deploy malware or ransomware and facilitate improved response and recovery from an attack. This new standard was filed with FERC on June 24, 2024, and is awaiting approval.

³² [Hitachi Energy Blames Data Breach on Zero-Day as Ransomware Gang Threatens Firm - SecurityWeek](#)

³³ [Nearly 1,000 Organizations, 60 Million Individuals Impacted by MOVEit Hack - SecurityWeek](#)

³⁴ [Johnson Controls Ransomware Attack: Data Theft Confirmed, Cost Exceeds \\$27 Million - SecurityWeek](#)

³⁵ [Industrial Giant ABB Confirms Ransomware Attack, Data Theft - SecurityWeek](#)

³⁶ [Energy giant Schneider Electric hit by Cactus ransomware attack](#)

³⁷ [Nearly 1,000 Organizations, 60 Million Individuals Impacted by MOVEit Hack - SecurityWeek](#)



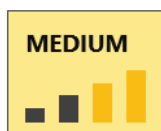
Scenarios

- A threat actor successfully ransoms systems on the general corporate network of a utility. They achieve limited impact on the bulk power system due to the segregation of operations from IT networks. A loss of corporate systems that support operations such as work management and purchasing cause a minor impact to power system operations, however, could result in business continuity challenges with prolonged restoration.
- A threat actor implants malware at a single low impact generation or transmission asset on the bulk power system, causing it to go out of service. This is a likely scenario because operational systems at those facilities typically have greater exposure to the internet.
- A threat actor delivered malware to the operational systems of a Balancing Authority or Transmission Operator and directly affected the ability to dispatch generation and operate transmission lines. There is a high impact on the reliability of the bulk power system, affecting most of the MRO region.

Actions to Reduce Risk

- Raise awareness of this risk with employees through phishing training, phishing tests, and follow-up activities when a user fails.
- Understand direct and indirect dependencies of systems on the general corporate network that support bulk power system operations and develop recovery plans to address outages of these systems.
- Maintain adequate backups of operational control systems and supporting systems and assess the security of backups to prevent corruption during an attack. Clean backups improve the chances of a successful recovery.
- Manage a large vector for this risk by limiting the use of email on operational control systems that support bulk power system operations.

Loss of Essential Reliability Services



Impact: Moderate

Likelihood: Possible

Essential reliability services (or ERS) refer to the frequency support, ramping and balancing, and voltage support required to maintain bulk power system reliability. Without ERS, the system would be at risk of collapse. These services are largely provided by a fleet of traditional, dispatchable power plants. Newer inverter-based and variable energy resources (i.e., wind and solar) do not provide the same level of ERS support as traditional power plants. As traditional power plants are phased out, and inverter-based and variable resources become more prevalent, ERS will be in shorter supply. System reliability is at risk unless alternative sources of required services are identified and installed in areas where they are needed. Quantifying the amount and location of needed ERS is not straightforward and requires in depth engineering analysis to plan for services properly.



Key Drivers

- The accelerated pace of retiring traditional power plants reduces the amount of ramping, balancing, and frequency/voltage support provided to the system.
- New generation interconnections are more dispersed and installed further from load centers, adding to grid voltage support requirements and requiring more individual generators to contribute to voltage support.
- IBRs have limited capability to provide ERS. Specifically:
 - wind and solar generation can only provide downward ramp unless they are operated sub optimally below their maximum capacity,
 - IBRs have little to no physical mass to stabilize frequency changes following a system disturbance. Systems with higher amounts of IBRs will experience larger frequency swings that may challenge system stability.
- Variable generation increases ramp requirements as large aggregations of weather-dependent resources collectively change system output. This is especially true for solar generation, which drives a large ramp down requirement in the morning and ramp up requirement in the evening.

Emerging Trends

- The 2024 NERC Long-term Reliability Assessment (LTRA) projects a net reduction of up to 25 GW of dispatchable generation over the next five years in portions of the MRO region.
- Ninety-five percent of MWs in the MISO and SPP interconnection queues are IBR, indicating most future generation development will be IBRs with limited capability to provide ERS.
- According to NERC's 2023 State of Reliability Report, the average monthly maximum contribution of wind and solar to meet total electricity demand in MISO and SPP grew 10% between 2021 and 2022, indicating periods with more wind and solar contribution than in the past.

Event History

- There have been no documented events from a lack of ERS.

Mandatory Controls

- NERC Reliability Standards BAL-001-2 (Real Power Balancing Control Performance), BAL-002-3 (Contingency Reserve for Recovery from a Balancing Contingency Event), BAL-003-2 (Frequency Response and Frequency Bias Setting), and BAL-005-1 (Balancing Authority Control) collectively are moderately effective at managing the real-time supply and demand balance required to maintain system frequency. However, these standards do little to address the transition of energy resources and the future ability of the system to balance supply and demand.
- NERC Reliability Standards PRC-010-2 (Undervoltage Load Shedding) and PRC-019-2 (Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection) are moderate controls requiring under voltage load shedding programs and coordination of voltage controls, respectively. However, both standards are designed around a system with large amounts of dispatchable generation and will become less effective as the system transitions to more IBR generation.



- NERC Reliability Standard VAR-002-4.1 (Generator Operation for Maintaining Network Voltage Schedules) is an effective control that requires generation, including IBRs, to provide voltage support on the system.

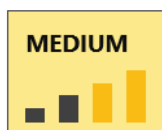
Scenarios

- Continued, accelerated retirement of coal and natural gas plants and growth in wind and solar plants leads to sharp increases in net load ramp requirements within a Balancing Authority. Increased ramp requirements exceed the ramp capability of online dispatchable resources, requiring load shedding to maintain generation and load balance during the ramp period.
- During a period of very high contribution of IBRs (~90%) within a Balancing Authority, the loss of the largest single generation contingency occurs, causing a steep decline in frequency. The limited response of online IBR generation causes an unstable recovery and results in additional generation and load tripping offline.
- A grid disturbance occurs in an area of large, inductive loads and multiple IBRs, causing a voltage collapse due to the lack of reactive power injection from local IBRs. This results in the need to shed load to restore normal system voltage.

Actions to Reduce Risk

- Resource planners need to manage the pace of dispatchable generation retirements that provide essential reliability services and coordinate with transmission planners to ensure required services are replaced before traditional plants are retired.
- Metrics need to be developed within long-term planning processes to determine the minimum required amounts of ramp capability, frequency response, and voltage control.
- Essential reliability services should be incentivized to meet the required levels of service expected in the future.
- Incorporate grid forming (GFM) technology in new battery systems to improve stability of the bulk power system, particularly in areas with high penetrations of IBRs.³⁸

Physical Attacks



Impact: Minor to Moderate

Likelihood: Possible to Likely

Physical Attack is the risk of a threat actor using lower cost and accessible means such as guns, bombs, drones, and vehicular impacts to damage high value or long lead time equipment, which may be located at critical facilities. Typical physical controls at most bulk power system facilities are fences, gates, locks, and cameras that are not effective at stopping determined attackers. Preventing physical attacks requires controls that deter, detect, and delay a threat actor. That combination reduces the probability of a threat actor targeting critical facilities and increases the time it takes for the attacker to reach critical equipment, providing more time for law enforcement to respond.

³⁸ https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_GFM_Functional_Specification.pdf

Key Drivers

- Elevated social and political unrest.
- Readily available public information on electrical infrastructure facilities to assist in planning an attack (e.g. – Google Maps).

Emerging Trends

In 2024, over 4,000 physical security incidents were shared to the E-ISAC by utilities across the U.S. and Canada. Figure 11 shows the breakdown of that number into activity types. The total number of attacks includes attacks on lower voltage distribution systems and the higher voltage bulk power system.

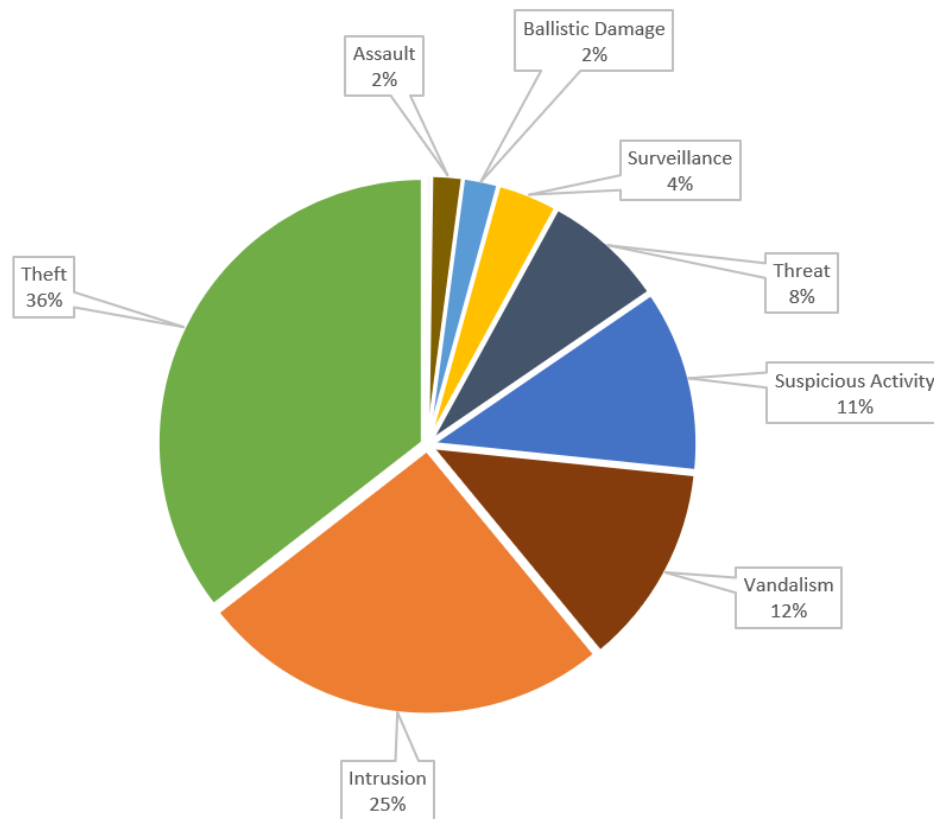


FIGURE 11 - 2024 E-ISAC REPORTED PHYSICAL INCIDENTS

- From 2023-2024, the most serious types of physical incidents leading to grid-impacts remain below three percent of the total shared.
- The tactics involved in incidents impacting the grid continue to be the result of ballistic damage, theft (copper), intrusion (tampering), and vandalism.
- There was an uptick in grid attacks in late 2022.
- In 2024, the E-ISAC observed an increase in copper theft and vandalism incidents in comparison to 2023



Event History

- A substation in North Dakota was attacked in May 2023 by ballistics, causing over \$100,000 in damage and impacting electrical distribution equipment that disrupted service to several hundred customers. The perpetrator was charged with destruction of an energy facility, which is punishable by a maximum term of 20 years and a \$250,000 fine.³⁹
- Two distribution substations in Moore County, North Carolina were attacked in December 2022 with ballistic damage to transformers and other equipment that led to 40,000 customers without power. A death that occurred due to the power outage was ruled a homicide.^{40,41}
- A plot to attack Baltimore, Maryland's power grid by an extremist with white supremacist ideologies in 2022 included plans to target five substations with a ballistic attack. The justice department estimates the attack could have caused up to \$75,000,000 in damages if successful. The perpetrator received 18 years in federal prison.^{42,43}

Mandatory Controls

- NERC Reliability Standard TPL-001-5.1 (Transmission System Planning Performance Requirements) establishes requirements for reliable operations of the Bulk Electric System over a wide range of probable contingencies. Physical attacks have largely targeted single power system elements (transmission lines, transformers, generators), which the system is designed to withstand as required by this standard. The power grid is highly resilient to physical attack because of its dispersed design.
- NERC Reliability Standard CIP-014-3 (Physical Security) is a moderately to highly effective standard for protecting critical facilities. It requires utilities to evaluate threats and vulnerabilities to physical attack and develop and implement a plan to reduce risk.
- NERC Reliability Standard CIP-006-6 (Physical Security of BES Cyber Systems) is a moderately effective standard for high and medium impact facilities. It requires organizations to establish a physical security perimeter around facilities and be aware of who breaches the perimeter. This provides some deterrence and often includes video surveillance, which aids in detection and investigation.

Scenarios

- Based on recent trends, threat actor(s) conduct a physical attack on one or two medium or high impact transmission or generation facilities. This impacts a single utility and affects a limited portion of the regional grid.
- A threat actor randomly targets bulk power system assets without intention to disrupt system operations (mainly by theft, intrusion, vandalism, or the occasional ballistics attack). These randomized attacks have limited impact to the regional bulk power system.

³⁹ [District of North Dakota | U.S. Attorney's Office Announces Arrest and Indictment of a Canadian Man for Destruction of an Energy Facility and Illegal Firearm Possession | United States Department of Justice](#)

⁴⁰ [What we know about the attack on two Moore County, N.C. power substations : NPR](#)

⁴¹ [Death of woman following attacks on North Carolina power stations ruled a homicide - ABC News](#)

⁴² [District of Maryland | Maryland Woman Pleads Guilty To Conspiring To Destroy The Baltimore Region Power Grid | United States Department of Justice](#)

⁴³ [White supremacist receives 18-year sentence for Baltimore power grid plot](#)



Actions to Reduce Risk

- Enhance deterrence to reduce the likelihood that assets will be targeted by a physical attack. Consider Crime Prevention Through Environmental Design (CPTED) principals during planning, site acquisition, engineering, and maintenance phases of a project.⁴⁴
- Understand the E-ISAC's Design Basis Threat for the electricity sector that defines reasonable and credible threat consideration, in combination with the Vulnerability of Integrated Security Analysis method to make informed, risk-based decisions on physical security upgrades.
- Develop engineering specifications for high-value, critical, long lead time equipment to increase resilience against gunfire.
- Subscribe to E-ISAC portal notifications. The E-ISAC will continue to closely monitor grid-impacting trends to keep the electric industry aware of any emerging threats.⁴⁵
- Build and maintain relationships with local law-enforcement to raise awareness that an attack on electrical infrastructure is not just a material crime but has greater impact to regional power grid reliability. Coordinate planning efforts with law enforcement to speed response in the event of an attack.
- Obfuscate publicly available surveillance data (e.g., Google Maps, openinfrastructure.org, etc.) as new facilities are brought online.
- Influence criminal penalties associated with destroying electrical infrastructure to increase the deterrent to potential threat actors.

Material and Equipment Availability



Impact: Minor

Likelihood: Possible to Likely

There is continued high demand to replace aging electrical equipment and support increased development of new generation and transmission facilities. The global manufacturing and supply chain of electrical equipment is strained beyond its capability to meet this demand. Lead times for many materials and equipment are well above historical norms, especially for critical components like circuit breakers, power transformers, and key networking equipment essential for protecting critical assets from cyber attack. Extended lead times limit the response time to replace failed or damaged equipment or address security vulnerabilities. Delays in equipment availability have broad reliability implications as system components may remain out-of-service for extended periods.

Key Drivers

- High global demand for electrical equipment to replace aging infrastructure and support the buildout of transmission and generation projects.
- Limited global production capability, especially of specialized equipment like large substation transformers.
- Ability to ramp production to meet increasing demand is limited as utilization rates are maxed out.

⁴⁴ [The International CPTED Association \(ICA\) - Primer in CPTED - What is CPTED?](#)

⁴⁵ <https://www.eisac.com/s/join-the-eisac>



Emerging Trends

- Lead times for large power system transformers increased from one to two years before the COVID-19 pandemic to more than five years in 2024.⁴⁶
- Lead times for transmission circuit breakers has increased from 6 months before to COVID-19 to four to five years in 2024.⁴⁶

Event History

- There have been no documented events attributed to lack of equipment availability, although multiple reliability-based construction projects have been delayed due to this risk.

Mandatory Controls

- NERC Reliability Standard TPL-001-5.1 (Transmission System Planning Performance Requirements) requires utility companies to have a plan in place for outages related to long equipment lead-times, which might include relying on shared spare equipment inventories. The standard requires an assessment of expected equipment lead times greater than one year, but does not require a firm solution to be in place to address the risk, limiting the standard's effectiveness.
- NERC Reliability Standards CIP-003-9 (Security Management Controls) and CIP-014-3 (Physical Security) set recovery plans and resiliency measures for cyber equipment protecting operational control systems. However, the standards are limited to equipment classified as a Bulk Electric System cyber systems and do not apply to all devices that are used in system operations, including transmission lines and substation transformers.

Scenarios

- Long delays in delivery of critical equipment like generation step-up transformers result in postponing in-service dates of several generation interconnections, which leads to inadequate generation capacity to meet demand.
- Delays in circuit breaker and transformer deliveries cause a major transmission project to be delayed past its need date, causing significant congestion on the bulk power system.
- Broad, severe storms traverse the MRO region and cause substantial damage to transmission line and substation facilities. Limited inventory of replacement materials lengthens restoration times, putting the bulk power system at risk to further failures including load loss.
- A physical attack results in the failure of multiple transmission transformers, severely constraining the bulk power system's ability to serve load and leading to extended outages because of equipment delays.

Actions to Reduce Risk

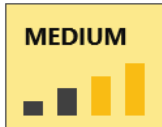
- Participate in spare equipment sharing programs to address unexpected failures of critical equipment.
- Develop and maintain good relationships with vendors of critical equipment to improve visibility and collaboration to address material and equipment shortages as they occur.

⁴⁶ [WAPA: Supply chains impact power transmission systems](#)



- Where possible, maintain higher levels of equipment inventory or have a well-established pipeline for equipment that may become in short supply or is needed due to unexpected failures.

Internet-Connected Devices



Impact: Moderate

Likelihood: Possible

Utilities are increasingly using internet-connected devices like smart meters, responsive load devices, and sensors on power lines to help manage the grid more efficiently. These devices don't directly control grid operations, but they still pose risk and are not subject to mandatory NERC Reliability Standards. The risk from internet-connected devices comes from the combined data from many devices as an input to bulk power system operations, and the ability to alter customer loads over a broad geographic area. These devices often operate outside the utility's direct control, creating more opportunities for threat actors to gain access and potentially disrupt grid operations.

Key Drivers

- A new aspect of power system operations is altering customer energy consumption as part of balancing the available energy from generators. Customer internet-connected devices (ex: smart thermostats, electric vehicle chargers) can be used to help control energy consumption, creating a new security risk for power system operations.
- Enhanced technology is being used to operate and plan the bulk power system to accommodate increased variability in supply and demand.
- The internet-connected devices used at customer locations will be connected to home and business networks. This presents a threat actor with many opportunities to affect the devices. This is insecure compared to the cyber protection provided to bulk power system equipment.

Emerging Trends

- According to the Edison Foundation, the projected installation of smart meters by 2026 is 142 million, which is an 80% increase from 2017.⁴⁷
- Both the industry and its regulators are interested in dynamic line rating sensors as a solution to increasing transmission line capacity.

⁴⁷ [IEI SmartMeterAtAGlance 2024 Update](#)



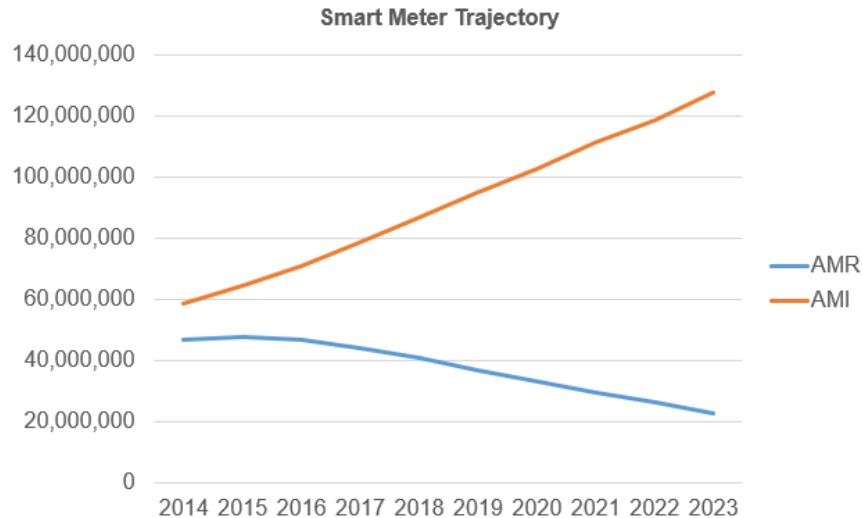


FIGURE 12 - SMART METER TRAJECTORY⁴⁸

Figure 12 shows the increase in Advanced Metering Infrastructure (AMI) and the decrease in Automatic Meter Reading (AMR). AMI meters have two-way communication and allow utilities and customers to interact and support smart consumption applications, as well as support responsive load and distributed generation. Older AMR meters only allow one-way communication for the utility to remotely read data from the meter. This graph shows how this technology transition is rapidly increasing the attack surface of internet-connected devices that can affect bulk power system operations.

Event History

- There are currently no documented events related to this risk.

Scenarios

- A threat actor manipulates control signals sent to millions of smart thermostats during a heat wave to simultaneously increase the amount of cooling load, exceeding the available ramp capability of generation and requiring operator-initiated load shedding to maintain system balance.
- A threat actor manipulates the data being sent from dynamic line rating sensors to reduce the rating of several transmission lines, which in turn notifies system operators of line overloads, requiring generation redispatch to maintain power flows below the artificially low limit.
- A threat actor manipulates power analog data at a third-party cloud Distributed Energy Resource (DER) aggregator, causing apparent generation imbalances. The situation causes operators to make ill-informed manual actions that cause system instability.

⁴⁸ Data for this graph was taken from eia.gov. [SAS Output](#)



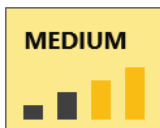
Mandatory Controls

- There are currently no NERC Reliability Standards that provide an effective control since most internet-connected devices are not classified by the CIP-002 standard as part of the Bulk Electric System.

Actions to Reduce Risk

- Consider system architecture changes to address the increase in internet-connected devices to minimize the impact that a combined number of compromised assets would have on the bulk power system.
- To bolster controls on data integrity, consider anomaly-based detection on control system values. This is in addition to integrity controls while data is in transit, such as hashing. This provides the ability to detect data manipulation while in-use.

Use of Inaccurate Transmission Facility Ratings



Impact: Moderate

Likelihood: Possible

Facility ratings dictate the maximum amount of power flow through a transmission facility. These ratings are based on year-round or seasonal assumptions of worst-case weather conditions to ensure equipment is not overloaded in the most extreme conditions. FERC Order 881, effective in 2025, requires that actual and near-term forecasted temperatures be used to determine facility ratings. This order substantially increases the amount of data required to develop and maintain accurate facility ratings because of the volume of assets and data required to set ratings and keep the assets and data current. Use of inaccurate facility ratings within operations or planning of the bulk power system can lead to equipment damage or require the need for load shedding.

Key Drivers

- The following are common challenges identified by the ERO Enterprise in sustaining accurate facility ratings⁴⁹
- Lack of awareness of installed equipment
- Inadequate asset and data management
- Inadequate change management
- Inconsistent development and application of facility rating methodologies
- FERC Order 881 will become effective in 2025 and requires use of ambient adjusted ratings for bulk power system facilities. This order requires a change in data management practices to increase the amount of data needed to calculate facility ratings, introducing potential inaccuracies.

49

<https://www.nerc.com/comm/RSTC/Documents/ERO%20Enterprise%20Themes%20and%20Best%20Practices%20for%20Sustaining%20Accurate%20FR%20-%20Final%20-%20Oct-20-22.pdf>



- Transformation of the grid to more dispersed and variable generation resources requires upgrading transmission line capacity and/or the construction of new transmission infrastructure. Inadequate change management for upgraded or new infrastructure increases the opportunity for error.

Emerging Trends

- Figure 13 reflects the top 10 most violated NERC Reliability Standards with moderate and serious risk in 2023. Violations of NERC Reliability Standards FAC-008 and FAC-009 had the most serious risk violations (seven out of ten) related to facility ratings. Serious risk violations are the highest designation in NERC’s Compliance Monitoring and Enforcement Program and indicate a severe impact to the bulk power system.

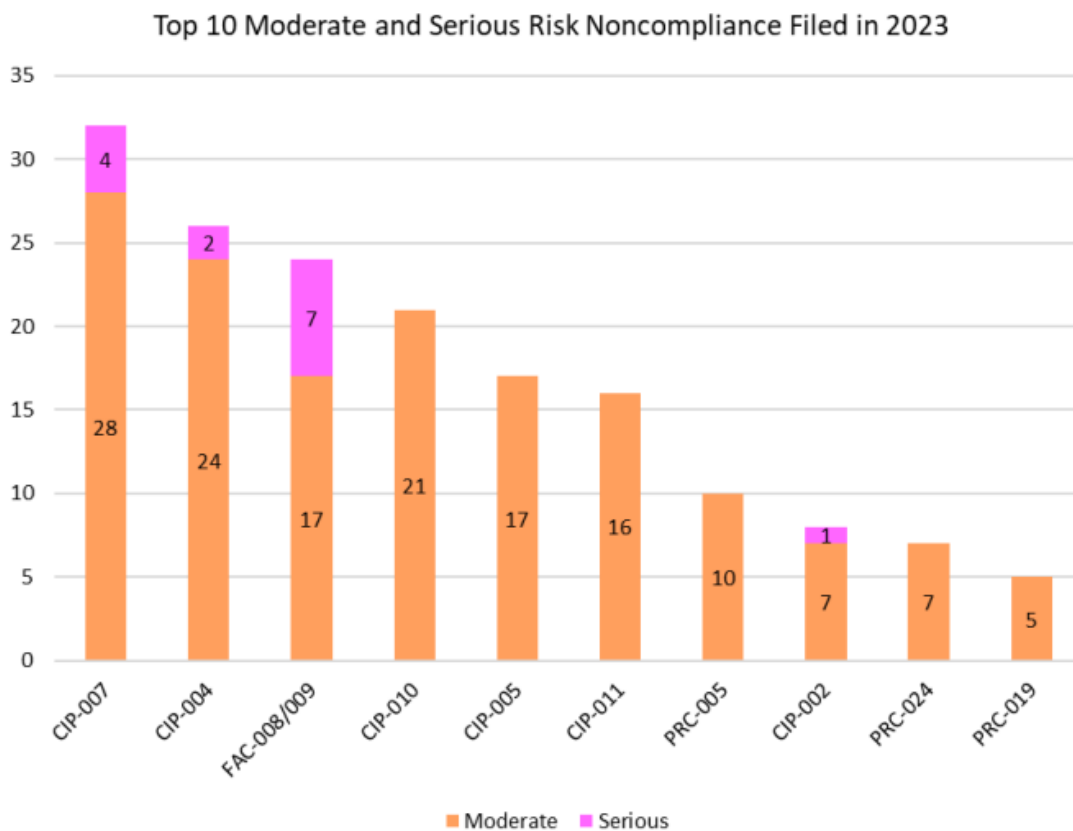


FIGURE 13 - SERIOUS AND MODERATE RISK NONCOMPLIANCE REPORTED IN 2023⁵⁰

- FERC Order 881 requires ambient-adjusted ratings to be calculated every hour from the current operating day to ten days out. Assuming most utilities use seasonal ratings, this increases facility rating calculations by 240 times, which substantially increases the possibility for error.

⁵⁰ [NERC 2024 Organization Registration and Certification Program and Compliance Monitoring and Enforcement Program Annual Report](#)



Event History

- A joint FERC/NERC report on the 2018 South Central US cold weather event⁵¹ noted the importance of accurate facility ratings in avoiding unnecessary generation redispatch or transmission reconfiguration and in providing more capacity to transfer power to resource-deficient areas.

Mandatory Controls

- NERC Reliability Standard FAC-008-5 (Facility Ratings) sets requirements for the determination of facility ratings based on technically sound principles. It is seen as a moderate control for this risk since the standard is focused on facility rating accuracy.

Scenarios

- An inaccurate facility rating on a transmission line serving a broad area of the MRO region is lower than the actual rating. A significant amount of generation output changes is needed to address the lower rating, which are beyond the capabilities of existing generation. To maintain power flow below the artificially low rating, system operators order load to be shed until other generation can be brought online.
- An inaccurate facility rating on a transmission line is higher than its actual rating, causing equipment on the line to fail due to the unidentified overload, resulting in loss of load served by the line.
- Use of static, year-round line ratings during an extreme cold weather event results in numerous overloads of different facilities and decisions by operators that result in operator-initiated load shedding to maintain loading below ratings that are not appropriate for the operating conditions.

Actions to Reduce Risk

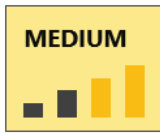
- Establish a sustainable facility ratings program that clearly documents processes and procedures and incorporates best practices from the ERO Enterprise report on *Themes and Best Practices for Sustaining Accurate Facility Ratings*.⁵² Support for the program needs to occur at all levels of an organization and deploy controls to test processes and procedures for effectiveness.
- While implementing FERC Order 881, develop strong processes and systems that enable expansion of data requirements for ambient-adjusted ratings to be accurately incorporated into existing operational systems.

⁵¹ https://www.nerc.com/pa/rrm/ea/Documents/South_Central_Cold_Weather_Event_FERC-NERC-Report_20190718.pdf

⁵² <https://www.nerc.com/comm/RSTC/Documents/ERO%20Enterprise%20Themes%20and%20Best%20Practices%20for%20Sustaining%20Accurate%20FR%20-%20Final%20-%20Oct-20-22.pdf>



Tight Supply of Expert Labor



Impact: Minor

Likelihood: Possible to Likely

Maintaining an experienced workforce is critical to navigating the challenges presented by the grid transformation. This has become increasingly more difficult due to a competitive job market, low unemployment, and the rapid evolution of grid technology. Insufficient staff expertise could impact grid reliability and prevent utility companies from preparing for future grid challenges.

Key Drivers

- Low unemployment rates in the U.S. and Canada.
- Growth in third-party companies like generation developers and companies looking to interconnect new loads to the grid are competing for expertise in bulk power system operations, planning, and security.

Emerging Trends

- There were 291,000 job openings in the transportation, warehousing, and utilities sector as of September 2024, which is down from the peak of 615,000 in January 2023, but higher than the five-year average of 238,000 between 2014 to 2019.⁵³
- According to [cyberseek.org](https://www.cyberseek.org), the number of job openings through August 2024 in cyber security was 457,398, compared to 720,727 in 2022 and 279,408 in 2014.

Event History

- There have been no documented bulk power system events related to a lack of expert employees.

Mandatory Controls

- There are no mandatory NERC Reliability Standards specifically addressing this risk.

Scenarios

- Persistent understaffing of personnel responsible for operations and planning of the bulk power system to maintain reliability leads to burnout of staff and an increase in mistakes that ultimately can affect reliability.
- Insufficient staff in cyber security results in fewer resources to monitor and respond to security threats, leading to some vulnerabilities not being addressed and diminishing overall system reliability.

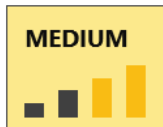
⁵³ <https://www.bls.gov/it/>



Actions to Reduce Risk

- Evaluate the workload of staff experts and where possible, redistribute work to less qualified individuals to allow experienced workers to focus on the highest-value activities.
- Establish strong training/mentoring programs to increase the skills and experience of all personnel.

Vulnerabilities of Unpatched Systems



Impact: Minor

Likelihood: Possible

One of the greatest cyber security risks is failing to address vulnerabilities in computer systems and software. These weaknesses are often exploited by threat actors to gain initial access to an organization’s network. In 2024, nearly 20 percent of all breaches across various industries were caused by exploiting known vulnerabilities. Often, a known vulnerability exists because a patch is not available or is difficult to apply, leaving those systems vulnerable to attack.

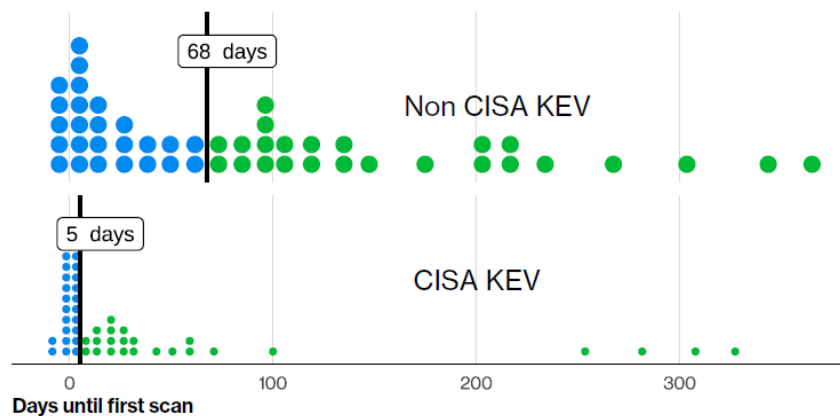


FIGURE 14 - TIME FROM PUBLICATION OF VULNERABILITY TO FIRST SCAN⁵⁴

Once a vulnerability is released publicly, on average an internet exposed system will see the first attempts to probe that vulnerability in 68 days. The Cybersecurity and Infrastructure Security Agency maintains a database of known exploited vulnerabilities (KEV), and internet exposed systems with vulnerabilities in that database see their first scans in 5 days as shown in Figure 14, proving that known vulnerabilities get exploited rapidly. The maturity of patch and vulnerability management programs within utilities and other defense in depth measures, particularly on operational control systems, limit the impact and likelihood of this risk. However, current drivers and trends show the frequency of known vulnerabilities are increasing, putting pressure on utilities to maintain adequate vulnerability management as the pace of change accelerates. Vulnerability management programs that are based primarily on patch notifications and minimum required mandated periodicity may not mitigate vulnerabilities rapidly enough, particularly when a vulnerability is in the CISA KEV database.

⁵⁴ 2024 Verizon Data Breach Incident Report



Key Drivers

- Patches on operational control systems are increasing in frequency and there is an expectation to push patches out in shorter timeframes without adequate time for assessment.
- Older legacy devices used to operate some equipment can no longer be patched.ⁱ
- Many less critical operational control systems remain exposed to the internet and are weakly protected.⁵⁵

Emerging Trends

- Since late 2023, Microsoft has observed an increase in reports of attacks focusing on internet-exposed, poorly secured operational control systems.
- Artificial Intelligence is increasingly used to help threat actors more quickly to leverage known vulnerabilities.
- Internet-facing VPN devices are used to secure data in operational control systems. These devices have been subject to increasing attack frequency.

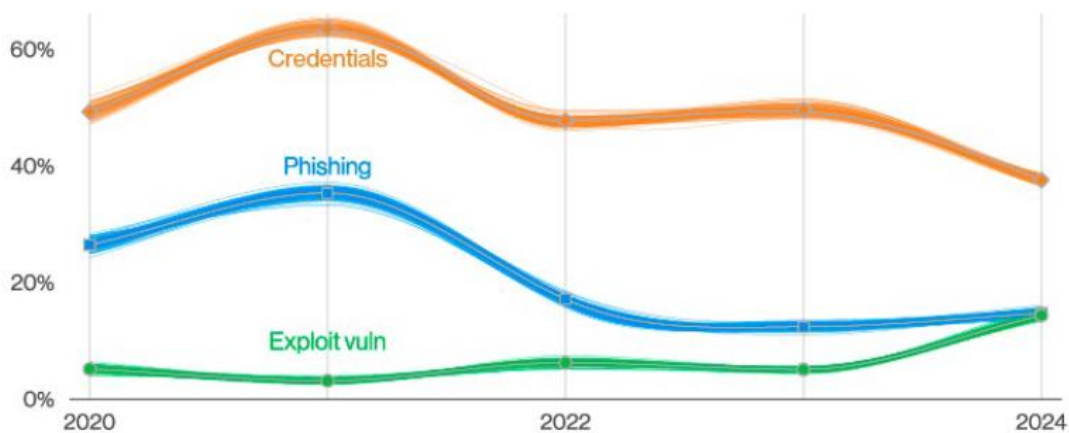


FIGURE 15 - TOP WAYS IN FOR NON-ERROR, NON-MISUSE BREACHES OVER TIME⁵⁶

Figure 15 shows across all sectors the prevalence of exploited vulnerabilities as the initial access method. The trends show a significant increase in 2024, nearly doubling the number of breaches attributed to exploited vulnerabilities over the numbers seen from 2020 through 2023. This bears continued monitoring in 2025.

⁵⁵ [Exposed and vulnerable: Recent attacks highlight critical need to protect internet-exposed OT devices | Microsoft Security Blog](#)

⁵⁶ 2024 Verizon Data Breach Incident Report



Event History

- The Danish Electric System was affected by an unpatched vulnerability in 2023⁵⁷. A critical patch for internet facing VPN devices was released on April 25, 2023, and 16 days later before it was applied, a threat actor launched a coordinated attack successfully gaining access to operational control systems at 11 energy companies. Despite the breach, there was no action taken by the threat actor to impact system operations.
- Commonly used internet-facing VPN devices had vulnerabilities under active exploitation prior to their discovery and public announcement. The vendor released mitigation tools, but they were ineffective at detecting compromise. Furthermore, the vulnerabilities allowed threat actors to gain and maintain access even on devices that had been reset and lay dormant. Patches were released over six months after initial discovery. Since this was a known vulnerability with an extended period before effective mitigation was available, some utilities made risk-based decisions to discontinue using affected equipment.^{58 59}

Mandatory Controls

- NERC Reliability Standard CIP-007-6 (System Security Management) contains requirements mandating patch management programs on medium and high impact assets that are moderately effective. Utility subject matter experts note, however, that the 70-day timeframe allowed between identification of a vulnerability and application of a patch may be too long.
- NERC Reliability Standard CIP-010-4 (Configuration Change Management and Vulnerability Assessments) subjects medium and high impact assets to vulnerability assessments as required by CIP-010. However, the 15-month required periodicity may not be timely enough to mitigate this risk.

Scenarios

- A threat actor utilizes an unpatched vulnerability to infiltrate and maintain persistence across many utilities and other supporting infrastructure due to the widespread deployment of common IT hardware across the utility industry. Extended outages of IT systems used to support core operations degrades the utilities' ability to respond to a physical or cyber event that targets operational equipment, causing a reliability challenge.
- A threat actor utilizes an unpatched vulnerability on internet-facing VPN devices to directly gain access to cyber systems used to control low impact generation sites at one utility. The threat actor uses this control to shut down these generation sites, impacting system reliability by requiring additional generation to come online or interrupting customer load to make up for the lost generation.
- A threat actor utilizes an unpatched vulnerability to compromise assets on the general corporate network of one utility. As a result, some systems are ransomed, which causes minor operational impacts to cyber systems used to control the bulk power system.

⁵⁷ [sektorcert-the-attack-against-danish-critical-infrastructure-ttp-clear.pdf](#)

⁵⁸ [Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways | CISA](#)

⁵⁹ [KB CVE-2023-46805 \(Authentication Bypass\) & CVE-2024-21887 \(Command Injection\) for Ivanti Connect Secure and Ivanti Policy Secure Gateways](#)



Actions to Reduce Risk

- Maintain compliance with prescriptive patch management requirements. Additionally, develop a risk-based framework for vulnerability management. Example factors to consider:
 - cyber asset criticality,
 - defense in depth measures that limit exposure,
 - other methods to mitigate the vulnerability,
 - incident response plans,
 - impact of the vulnerability,
 - age of the vulnerability, and
 - if the vulnerability is known to be exploited in the wild.

6. CONCLUSION

The North American bulk power system provides a critical service to the quality of modern life, supporting the economy, national security, and public health and safety. This complex system must remain reliable and secure to meet the growing dependence society has on electricity. Identification and prioritization of risk through MRO's Regional Risk Assessment is the first step in determining the areas of focus for maintaining reliability and security of the bulk power system in our region.

Collaborating and coordinating with industry stakeholders to develop and implement necessary actions to address the prioritized risks will ensure that the most pressing risks are mitigated before impacts occur.

The 2025 RRA supports MRO's mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system within the region. It establishes the foundation for MRO's risk monitoring and mitigation work and ensures efforts and resources are focused on the risks that are most critical.

MRO will continue to play a key role in studying, understanding, and communicating the reliability impacts associated with these challenges to advance our vision of a highly reliable and secure North American bulk power system.



7. REFERENCES

1. 2023 ERO Reliability Risk Priorities Report
https://www.nerc.com/comm/RISC/Related%20Files%20DL/RISC_ERO_Priorities_Report_2023_Board_Approved_Aug_17_2023.pdf
2. MRO Reliability Risk Matrix
<https://www.mro.net/document/mro-reliability-risk-matrix-2021/>
3. 2023 NERC State of Reliability Technical Assessment
https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2023_Technical_Assessment.pdf
4. 2024 NERC State of Reliability Technical Assessment
https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2024_Technical_Assessment.pdf
5. 2024 NERC Long-Term Reliability Assessment
https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_Long%20Term%20Reliability%20Assessment_2024.pdf
6. NERC Event Analysis Program
<https://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx>
7. 2024 MRO Regional Summer Assessment
<https://www.mro.net/document/mro-2024-regional-summer-assessment/?download>
8. 2024/2025 MRO Regional Winter Assessment
<https://www.mro.net/document/mro-2024-regional-winter-assessment/?download>
9. NERC 2024 Summer Reliability Assessment
https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2024.pdf
10. NERC 2024-2025 Winter Reliability Assessment
https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_WRA_2024.pdf
11. NERC/FERC January 17, 2018 Cold Weather Event Inquiry Report
<https://www.ferc.gov/legal/staff-reports/2019/07-18-19-ferc-nerc-report.pdf>
12. NERC/FERC/RE February 2021 Cold Weather Outages in Texas and the South Central United States Report
<https://www.ferc.gov/media/february-2021-cold-weather-outages-texas-and-south-central-united-states-ferc-nerc-and>
13. NERC/FERC/RE December 2022 Winter Storm Elliott Report
<https://www.ferc.gov/media/winter-storm-elliott-report-inquiry-bulk-power-system-operations-during-december-2022>
14. MRO Generator Winterization Program
<https://www.mro.net/program-areas/reliability-analysis/generator-winterization-program/>

