Statement of the North American Electric Reliability Corporation
2021 Annual Reliability Technical Conference
Docket No. AD21-11-00
September 30, 2021

I. Introduction

The North American bulk-power system (BPS) is undergoing major transformation, driven by a rapidly changing generation resource mix. Traditional baseload generation plants are retiring, while significant amounts of new natural gas and variable energy generating resources are being developed. During this transition, natural gas-fired generation is becoming more critical to provide both "bulk energy" and "balancing energy" to support the integration of variable energy resources. Extreme weather exacerbates the challenges of the transforming grid while also stressing the system in unique ways. Further, extreme weather or other stresses on related critical infrastructures, such as the natural gas system that the electric system depends upon, can impact the reliable operation of the BPS. Amid this rapid transformation, security threats continue to evolve in sophistication, frequency, and scope and pose ever-increasing risks to reliability and resilience. In what can only be described as extraordinary, the past year has seen the manifestation of each of these risks, all while industry continues to navigate the challenges of the ongoing global pandemic. The importance of electricity to the lives of nearly four hundred million North Americans is also ever increasing, being a fundamental enabler of their way of life.

NERC is pleased to discuss the work that it is undertaking to address these risks, with special emphasis on the changing resource mix, including the increasing penetration of inverter-based resources, the challenges of extreme weather, and cyber security risks.

II. 2021 State of Reliability

With a highly reliable and secure BPS at the core of NERC's mission, NERC is focused on proactively addressing the reliability risks of the transforming grid. In furtherance of its mission, NERC's *State of Reliability* report assesses the annual performance of the BPS. This report provides objective and concise information to policymakers, industry leaders, and the NERC Board of Trustees on issues that affect the reliability, resilience, and security of the North American BPS. By analyzing BPS performance through a number of datasets collected over the previous year, the report identifies system performance trends and emerging reliability risks, reports on the relative health of the interconnected system, and measures the success of mitigation activities deployed.

2021 State of Reliability was published on August 17, 2021.[1] The report finds that in 2020, North America's BPS faced numerous challenges, including extreme weather, cyber and physical threats, and a rapidly changing generation resource mix, all within the context of a global pandemic. Despite these challenges, the system continued to perform well, showing no cascading instability or uncontrolled separation, continued reduction in the misoperations rate, improving transmission outage restoration after extreme weather, and a reduction in transmission outages caused or initiated by human error.

Among unfavorable trends, operator-initiated load shedding increased in 2020, largely due to impacts from major extreme weather events: Hurricane Laura in the Gulf Coast, the California August heat wave, and the October ice storm in Texas. Absent those events, BPS performance would have been on par with previous years. Collectively, weather events and wildfires caused transmission outages with greater frequency than in prior years and were contributors to the most widespread outages.

[1] NERC, 2021 State of Reliability (Aug. 2021), available at https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2021.pdf

In Texas and parts of the Western Interconnection, energy and resource adequacy issues escalated in 2020. Local energy-assured generation remains necessary for reliability and resilience. The projected capacity deficit in Texas remained a reliability risk in 2020; however, mild weather and better-than-expected performance from the generation fleet, coupled with aggressive demand-side management and price response, helped Texas meet its 2020 summer peak demand. Texas now depends on significant contributions from variable energy and demand-side resources to meet peak demand. The risk of resource shortfalls is no longer restricted to the summer peak demand periods and must now be anticipated during shoulder months and the winter. NERC's winter seasonal reliability assessment[2] identified potential Energy Emergency Alert risk in parts of North America, including Texas and parts of the Western Interconnection, due to extreme weather, fuel, and energy issues.

In 2020, as in years past, no reportable cyber security incidents were identified that resulted in a loss of load under the CIP-008-5 standard. However, the increase in frequency and sophistication of attacks is well recognized, including from nation state adversaries and organized cyber-criminals with demonstrated capability to disrupt critical infrastructure, including the electricity sector. The *2021 Annual Threat Assessment* identifies acute cyber threats from China, Russia, Iran, North Korea, and their surrogates.[3]

Increased vulnerability disclosures by security and equipment vendors and increased voluntary sharing by entities gave the E-ISAC greater insight into the cyber security threat environment. Sharing of cyber security information on the E-ISAC's secure portal increased by

---

[2] See report at https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC%20WRA%202019_2020.pdf

[3] See report at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

96% in 2020 compared to 2019, leading to greater industry awareness of threats. Furthermore, the pandemic created an increased remote cyber security attack surface for industry due to increased telework. This required greater sharing and collaboration by the E-ISAC with all levels of the electricity industry, United States and Canadian governments, and partners than ever before.

The E-ISAC notes a significant increase in critical vulnerabilities in enterprise software and operational technology (OT/ICS) platforms. Accordingly, the SolarWinds supply chain compromise discovered in December 2020 keeps cyber security in the forefront of industry security and resilience planning. NERC and industry must maintain a continued focus on improving defenses by increased sharing with the E-ISAC. Industry must also adapt to a threat landscape where adversaries adopt new tactics, new vulnerabilities are exploited, and the magnitude of potential impacts are changing as the grid evolves and cross-sector interdependencies increase.

As mentioned previously, the global pandemic posed unique challenges for reliability. Due to advance planning, careful coordination across industry participants and with government partners, and a keen focus on risk, industry demonstrated remarkable resilience in navigating myriad challenges. While the full impact of the pandemic will not be known for some time, there is no evidence to suggest that it adversely affected BPS reliability in 2020. Instead, there is ample evidence to suggest that advance planning by industry and the consistent execution of these plans were highly successful in addressing the unprecedented reliability operating challenges caused by the pandemic. In the spring of 2020, NERC issued a *Special Report: Pandemic Preparedness and Operational Assessment*.[4] Additionally, the North American Transmission Forum, NERC, the U.S.

[4]

Department of Energy (DOE), and FERC jointly developed the *Epidemic/Pandemic Response Plan Resource*[5] to complement an organization's business or operations continuity plans with a focus on activities that are specific to the outbreak of a severe epidemic/pandemic. Finally, NERC played an important role in developing the ESCC's pandemic resource guide, largely admired as an essential reference document across multiple sectors.

2021 State of Reliability includes several key recommendations, summarized here:

- The ERO and industry should continue improving their ability to model, plan, and operate a system with a significantly different resource mix.

- System planners should evaluate the need for flexibility as conventional generation retirements are considered by industry and policymakers. Retirement planning studies should consider Interconnection level impacts and sensitivity assessments associated with the loss of critical transmission paths and the loss of local generation in larger load pockets.

- The ERO and industry should develop comparative measurements and metrics to understand the different dimensions of resilience during the most extreme events and how system performance varies with changing conditions.

- The ERO, industry and government should significantly increase the speed and detail of cyber and physical security threat information sharing in order to counter the increasingly complex and targeted attacks by capable nation-state adversaries and criminals. This should be complemented by a review of cyber security standards, supply chain procurement, risk assessment as well as a reviewing if the CIP standard's bright-line criteria between high-, medium-, or low-impact assets is sufficiently robust against the sophisticated supply chain attacks seen over the past 10 months.
- Further, system designs need to be evaluated and cyber robust designs deployed to improve the security and resilience of the BPS.

III. 2021 ERO Reliability Risk Priorities Report

NERC, Special Report: Pandemic Preparedness and Operational Assessment (Spring 2020), https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERC_Pandemic_Preparedness_and_Op_Assessment_Spring_2020.pdf.

[5] See report at https://www.natf.net/documents.

Every two years, the NERC Reliability Issues Steering Committee prepares a report to strategically identify, define, and prioritize risks to the reliable operation of the BPS and provide recommendations to the NERC Board of Trustees regarding the approach that NERC, the ERO Enterprise, and industry should take to enhance reliability and manage those risks. The *2021 ERO Reliability Risk Priorities Report* ("RISC Report") was approved by the NERC Board of Trustees on August 12, 2021.[6] It is a forward-looking view of imminent and projected risks to BPS reliability.

For 2021, the RISC Report defines eleven major risks to reliability, with the top four being: (1) grid transformation; (2) security; (3) extreme events; and (4) critical infrastructure interdependencies. In order of priority, the RISC report defines the following risks, listed in order of priority:

- Changing resource mix
- Cyber security vulnerabilities
- Resource adequacy and performance
- Critical infrastructure interdependencies
- Loss of situational awareness
- Extreme natural events
- Physical security vulnerabilities
- Bulk-Power System planning
- Control and protection systems complexity
- Human performance and skilled workforce
- Electromagnetic pulse

IV. Extreme Weather, Risks and Challenges

As NERC emphasized in its comments in the Climate Change, Extreme Weather, and Electric System Reliability Technical Conference docket,[7] extreme events are having greater

[6] See report at https://www.nerc.com/comm/RISC/Documents/RISC%20ERO%20Priorities%20Report_Final_RISC_Approved_July_8_2021_Board_Submitted_Copy.pdf

[7] *See Comments of the North American Electric Reliability Corporation*, Docket No. AD21-13-000 (Mar. 15, 2021).

impacts on the reliability of the BPS, and these impacts are largely attributable to impact of extreme weather on the rapidly transforming grid. NERC's most recent assessments have warned of the potential for the loss of large amounts of generating resources due to severe weather in winter and summer, and the potential need for grid operators to employ operating mitigations or Energy Emergency Alerts ("EEAs") to meet energy and peak demand.[8] NERC's assessments have highlighted that during extreme and prolonged winter conditions, vital natural-gas fuel supplies for electricity generation can be at risk in New England, California and the southwestern United States. While sufficient *capacity* may be available, the ability to provide *energy* during these extreme and prolonged winter conditions may be challenging. High reliance on natural gas-fired generation and limited natural gas infrastructure and competing needs for scarce molecules elevates reliability risk in some of these areas, impacting BPS resilience. In other cases, issues with plant winterization or disruption in electric loads used to winterize or drive natural gas production and transportation elevates the risk. With proper planning, including consideration not only of historic temperature averages but also consideration of evolving conditions during extreme weather events, seasonal and rolling operational energy planning, and the linkage between critical infrastructures, the risks associated with extreme weather and the changing resource mix could be mitigated.

The Commission recently approved a suite of revised Reliability Standards to address the reliability risks posed by cold weather: Reliability Standards EOP-011-2 (Emergency Preparedness and Operations); IRO-010-4 (Reliability Coordinator Data Specification and

---

[8] *See, e.g.*, NERC, *2020-2021 Winter Reliability Assessment* (Nov. 2020), https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_WRA_2020_2021.pdf; NERC, *2020 Summer Reliability Assessment* (June 2020), https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_SRA_2020.pdf

Collection), and TOP-003-5 (Operational Reliability Data) (collectively, the "Cold Weather Reliability Standards"). Before the most recent cold weather event in Texas and the South Central United States in February 2021, extreme cold weather events caused substantial reliability and resilience impacts in 2011, 2014, and 2018. The fact that four such events occurred over the past decade demonstrates that these events can no longer be treated as rare. Further, in the past decade, the generation fleet has transformed to one that is more sensitive to weather with extreme temperatures. As discussed in NERC's petition for approval,[9] the Cold Weather Reliability Standards would advance BPS reliability by requiring generators to implement plans for cold weather preparedness. Additionally, the Cold Weather Reliability Standards would enhance the ability of the Balancing Authority, Transmission Operator, and Reliability Coordinator to plan and operate the grid reliably during cold weather conditions by requiring the exchange of information related to the generator's capability to operate.

While approval of the Cold Weather Reliability Standards mark an important milestone, NERC is continuing and expanding upon work to address extreme weather risks before the standards become mandatory and enforceable in 2023. NERC and the Regional Entities are now in the process of conducting substantial winter weather readiness outreach and training to entities, expanding upon efforts from prior years. On August 18, 2021, NERC issued a Level 2 Alert[10] containing recommended actions for winter weather preparedness.[11] The responses to the

---

[9] *Petition of NERC for Approval of Proposed Reliability Standards EOP-011-2, IRO-010-4, and TOP-003-5*, Docket No. RD21-5-000 (Jun. 17, 2021).

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

[11] The NERC Alert system is described in Section 810 of the NERC Rules of Procedure and includes three levels: Level 1 (Advisories), Level 2 (Recommendations) and Level 3 (Essential Actions). Level 2 and Level 3 Alerts require responsive action and reporting by the receiving entities. Before issuing an Alert, NERC must provide the Commission with at least five business days' notice. Following the issuance of a Level 2 or Level 3 Alert, NERC is responsible for filing a report to the Commission summarizing the actions taken and the success of such actions in correcting any vulnerability or deficiency that was the subject of the notification. See NERC Rules of Procedure

Level 2 Alert will inform industry follow-up throughout the ERO Enterprise and assessed in NERC's upcoming Winter Reliability Assessment. Responses will also help inform further analysis, and reporting. The work of the joint FERC, NERC, and Regional Entity inquiry into the causes of the February 2021 event affecting Texas and the South Central United States is nearing its completion, and NERC is prepared to act promptly on any additional recommendations for standards modifications arising from the joint inquiry.

With respect to extreme weather more generally, NERC staff will continue to examine the Reliability Standards to determine if other modifications are needed. Presently, Reliability Standard TPL-001-4 requires planning entities to study wide area events affecting the transmission system caused by loss of generating stations due to factors such as wildfires and severe weather.[12] Additional modifications may be appropriate to address fuel concerns during extreme weather conditions. NERC's assessments and the results of the FERC/ERO Enterprise joint inquiry into the causes of the February 2021 cold weather event may provide additional considerations for Reliability Standards enhancements. Such enhancements could include:

- Reliability Standard requirements that establish a process for determining the ambient temperature and weather conditions to which plants must weatherize.
- Reliability Standard requirements for the Generator Owner to identify and implement freeze protection measures for cold-weather-critical components and systems, and for Generator Owners to develop and implement Corrective Action Plans when their facilities experience outages, failures to start, or derates due to freezing.
- Reliability Standard requirements and seasonal assessment protocols that better account for expected generator availability during cold weather, taking into account factors such as contractual arrangements for natural gas supply.

Section 810, Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions. The NERC Rules of Procedure are available at https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx.

[12] Reliability Standard TPL-001-4 – Transmission System Planning Performance Requirements, https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-001-4.pdf. In January 2020, the Commission issued Order No. 867 approving Reliability Standard TPL-001-5. *See Transmission Planning Reliability Standard TPL-001-5*, Order No. 867, 170 FERC ¶ 61,030 (2020). Reliability Standard TPL-001-5 will become effective in accordance with its phased-in implementation plan on July 1, 2023.

- Reliability Standard requirements to protect critical natural gas infrastructure from manual and automatic load shedding, to avoid adversely affecting BPS reliability.

- Reliability Standard requirements for the Reliability Coordinator, Balancing Authority, or Planning Coordinator to determine the temperature to which plants in their respective areas must weatherize.

- Reliability Standard requirements for the Reliability Coordinator or Balancing Authority to develop seasonal emergency energy management plans, to address conditions such as wildfires, extreme hot and cold temperatures, and severe storms (i.e. hurricanes).

- Reliability Standard requirements for the Reliability Coordinator to develop a rolling three week emergency energy management plan.

- Reliability Standard for the development of a Seasonal Energy Management Plan based on regional extreme weather scenarios, to be assessed as part of NERC's seasonal assessments, and to include weatherization, fuel availability, projected unit maintenance, electric supply to gas wellheads and compressors, operating procedure, and so on; and a determination of the sources of energy and the degree of certainty with each source.

Numerous NERC reliability assessments identify natural gas fuel supply as a growing risk to BPS reliability due to the effects of extreme weather. The BPS is becoming increasingly reliant on natural gas for electric generation. Unlike generation with on-site fuel storage, natural-gas-fired generators depend on the natural gas pipeline system to deliver just-in-time fuel for electricity production. Unless they are dual-fuel units with onsite fuel oil or have local natural gas, CNG or LNG storage, they can be particularly sensitive to extreme cold temperature, and should be winterized to reduce the risk to their ability to operate. Likewise, the natural gas system is also sensitive to extreme weather conditions. Further, growth in demand for natural gas as a fuel for electric generation and other applications can stress the natural gas supply infrastructure when necessary expansions (i.e. additional pipelines and storage) do not keep pace. While natural gas disruptions could cause reliability and resilience impacts at any time of the year, the problem is particularly acute during extreme weather conditions. These impacts can be further exacerbated by the loss of electricity, as natural gas wellheads, processing plants and compressors may be winterized and powered by electricity.

Planning considerations can help mitigate natural gas fuel risks.[13] However, the natural gas system was not built to primarily serve the needs of an electric power sector that is increasingly dependent upon reliable natural gas service, nor is it regulated or operated as such. When it comes to BPS reliability, NERC believes the current framework for regulation and oversight of natural gas supply for electric generation needs to be rethought. Clear regulatory authority is needed over natural gas when used for electric generation to help support BPS reliability and resilience.

In examining potential Reliability Standards enhancements, NERC looks to those that can be applied using NERC's principles for performance-based standards. NERC looks forward to continued discussion in this proceeding and the Climate Change, Extreme Weather, and Electric System Reliability technical conference docket (Docket No. AD21-13-000) regarding Reliability Standards enhancements that may help address the reliability risks posed by extreme weather.

V. Maintaining Reliability with Changing Resource Mix

A. NERC's Holistic Approach to Addressing Risks to BPS Reliability

NERC's efforts to maintain reliability under a constantly transforming resource mix illustrates the ERO Enterprise's holistic technically focused approach to addressing risks to BPS reliability. The NERC RSTC is leading many projects to address different challenges presented by the changing resource mix, which features (1) increasing penetration of asynchronous inverter-based resources, (2) growing levels of distributed energy resources (DERs), and (3) retirement of centralized synchronous generation.

NERC's multi-faceted approach to evaluating the risks presented by the transforming resource mix includes particular focus on the rapid growth of inverter-based resources (IBRs)

[13] *See, e.g.*, NERC, *2020 Long-Term Reliability Assessment* at 34.

and DERs. This includes analysis of grid events which led to the development of reliability guidelines, technical reports, webinars, workshops, and standard authorization requests. NERC has initiated Alerts to understand the extent of condition of various reliability issues identified in the reports, and has continued to evaluate IBR performance across multiple interconnections. The RSTC subgroups have also developed multiple SARs to bring clarity and consistency to inverter-based BES resources within the existing standards realm.

This work is accomplished with the help of several RSTC subgroups, working groups, and task forces. In particular, the NERC Inverter-Based Resource Performance Working Group (IRPWG) has been instrumental in helping drive recommended practices through NERC Reliability Guidelines to support the reliable interconnection of inverter-based resources connected to the BPS. In 2020, for example, NERC published, *Reliability Guideline: Performance, Modeling, and Simulations of BPS Connected Battery Energy Storage Systems [BESS] and Hybrid Power Plants* to help support the growing levels of BESS and hybrid plants connecting to the BPS.[14] The IRPWG also published two guidelines in 2018 and 2019 focused on recommended performance characteristics for all BPS-connected inverter-based resources and recommendations for all Transmission Owners, Transmission Planners, and Planning Coordinators to improve their interconnection requirements and study processes to support reliable integration of these resources.[15,16] These guidelines were issued in tandem with Alerts posted to address systemic performance issues identified with solar PV resources, in particular, after the Blue Cut Fire and

[14] Available at https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_BESS_Hybrid_Performance_Modeling_Studies_2020-12-15%20(003).pdf.

[15] See https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Inverter-Based_Resource_Performance_Guideline.pdf.

[16] See https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf.

Canyon 2 Fire disturbances involving widespread reductions of solar PV resources in California. Since then, NERC has analyzed three additional widespread solar PV reduction events in California and one large event in Texas. California has recently experienced an additional four solar PV-related events that NERC and WECC are currently analyzing. The ERO Enterprise also published a compliance practice guide in 2021 to provide guidance to ERO Enterprise staff with respect to the consistent application of the BES Definition and NERC Registry Criteria to battery energy storage systems.[17]

In 2021, the System Planning Impacts from Distributed Energy Resources Working Group ("SPIDERWG") of the RSTC developed a draft Reliability Guideline on impacts that higher penetration of DER may have on Underfrequency Load Shedding. In June of 2021, the RSTC approved posting of this guideline for comment. The SPIDERWG is also presently working on a whitepaper examining BPS considerations associated with increasing participation of aggregated DER in wholesale markets.

NERC is carefully scrutinizing energy adequacy across the BPS. The Energy Reliability Assessments Task Force ("ERATF") under the RSTC is assessing risks associated with unassured energy supplies, including the timing and inconsistent output from variable renewable energy resources, fuel location, impact on resilience, and volatility in forecasted load, which can result in insufficient amounts of energy on the system to serve electrical demand. The ERATF provides a formal process to analyze and collaborate with existing groups reporting to the RSTC, and stakeholders to address the issues identified in the whitepaper, "Ensuring Energy Adequacy with Energy-Constrained Resources."[18] The whitepaper identifies energy availability concerns related

[17] *ERO Enterprise CMEP Practice Guide: Application of the Bulk Electric System Definition to Battery Energy Storage Systems and Hybrid Resources* (Feb. 2021).

[18] Available at https://www.nerc.com/comm/RSTC/ERATF/ERATF%20Energy%20Adequacy%20White%20Paper.pdf.

to operations/operations planning and mid- to long-term planning horizons. To address challenges presented by the changing resource mix, NERC encourages participation in RSTC and Reliability Standard initiatives.

To prioritize and monitor risk mitigations, NERC is developing an ERO risk registry and heat maps that encompass prior RISC report findings, and ongoing technical committee activities. This registry was completed at the end of the third quarter of 2021. Work plans of the technical committees will then be periodically reviewed to ensure that ongoing activities are tied to identified risks in the risk registry. Furthermore, if new risks emerge, they can be added to the registry, and if risks are being sufficiently mitigated, they will be moved to the monitored portion of the risk registry. A risk prioritization process is being developed in collaboration with RISC and RSTC. As the RSTC develops its annual work plan, and with the RISC biennial risk report now finished, the RISC and RSTC will review the risk registry to evaluate how completed work addressed these identified risks, whether any new risks have been identified by either committee that need to be added to the registry, any risk prioritization required, and document monitored risks that require no additional mitigation.

The discussion below focuses on several additional questions listed for Panel 4 in the Supplemental Notice of Technical Conference:

B. IBR Integration

As more IBRs are deployed, it is increasingly important that they connect to the BPS in a reliable manner. Recent events are cause for concern. For example, in May and June 2021, Texas experienced widespread reduction of over 1,100 MW of solar PV generation similar to those previously identified in California. Described as the "Odessa Disturbance," the causes of abnormal performance stem from the lack of adequate performance requirements and insufficient

modeling and studies at the time of interconnection. Full details of the Odessa Disturbance event, including key findings and recommendations, are covered in the report. "Texas Events: May 9, 2021 and June 26, 2021 Joint NERC and Texas RE Staff Report."[19]

IBR resources continue to seek faster interconnection times with abbreviated processes; however these objectives must be balanced with reliability and resilience. NERC is committed to working with its stakeholders and FERC to develop solutions to ensure that these resources are interconnected in a reliable and secure manner. This includes:

Generator Interconnection Processes – NERC recommends that FERC modernize its Generator Interconnection Procedures to improve (1) detailed data and modeling of all newly connecting resources (including updates to the requirements for inverter-based resources), and (2) the extent of studies performed by transmission service providers to ensure that resources are interconnected in a manner that balances efficiency of the interconnection process with reliability of the grid.

Reliability Standards – NERC is pursuing modifications to Reliability Standards to respond to these new risks posed to BPS reliability due to the changing resource mix. This includes evaluating current standards, whether new or modified standards are warranted, or if existing standards should be retired. Considerations include:

- A performance validation standard that enables transmission entities (TOPs, RCs, BAs, etc.) to seek corrective actions from plants not meeting established performance requirements at the time of interconnection. The FAC-001 and FAC-002 standards do not include such after-the-fact validation of performance and corrective actions to abnormal performance issues. This has led to systemic performance issues only being identified when large disturbances are identified by the ERO Enterprise rather than a proactive

[19] See report at https://www.nerc.com/pa/rrm/ea/Documents/Odessa_Disturbance_Report.pdf.

industry-driven approach to addressing these issues before more widespread disturbances occur.

- Potential modification of PRC-024 to comprehensively ensure generating resource ride-through to grid disturbance events. Recent revisions were made to PRC-024 to add clarity and prevent misinterpretation, but ongoing work by the ERO Enterprise demonstrates that this standard is not providing sufficient protection to avoid abnormal IBR performance issues. Many of the causes of power reduction from inverter based resources analyzed by the ERO Enterprise are also not addressed by the existing requirements of PRC-024 (i.e., not related to voltage or frequency protection or controls).

- Consideration of developing IBR-specific standards or requirements. The goal is not to impose unnecessary requirements on these types of resources. Rather, it is to bring clarity and consistency to the industry on how to effectively meet performance needs. And given the increasing deployment of IBRs (particularly solar PV and batteries), establishing clear requirements will be of increasing importance. Recognizing NERC's fuel/technology neutrality, we must acknowledge that current standard drafting teams are struggling with how to write standards suitable to different types of resources, and additional clarity may be needed in the form of specific requirements. The transformation of the grid has resulted in asynchronous IBR with controls that both support and impact the reliable operation of the BPS. The characteristics of these resources are much different than they are for synchronous machines. This gets further complicated with the introduction of hybrid power plants where multiple forms of generation and battery energy storage are coupled together as one asset.

Guidelines – NERC published foundational reliability guidelines related to BPS-connected inverter-based resource performance and requirements in 2018[20] and 2019.[21] These guidelines were shared broadly across industry with strong recommendations to be comprehensively adopted by industry. These guidelines are some of the most accessed materials published by NERC in recent years and there are countless webinars, workshops, and other industry engagements where these materials have been shared. Further, these materials were a catalyst of version 1 of the IEEE P2800 activities seeking to provide equipment standardization and

[20] See https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Inverter-Based_Resource_Performance_Guideline.pdf

[21] See https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_IBR_Interconnection_Requirements_Improvements.pdf.

interoperability for BPS-connected IBRs. That said, the recent events in Texas demonstrate that guidelines alone may not be sufficient to drive the needed industry response.

NERC continues to support industry efforts and analyze the extent to which the guidelines are being adopted by industry and consistent with the process described in connection with NERC's last Performance Assessment will review the effectiveness and efficiency of guidelines under the leadership of the RSTC.

Models and Studies – NERC continues to support industry efforts to improve modeling of inverter-based resources. NERC has published multiple guidelines, technical reports, white papers, and its own independent assessments of model quality. These materials document modeling issues in the positive sequence dynamic models used by grid planners for performing reliability studies. Further, as flagged above in connection with FERC's Generator Interconnection Procedures, NERC recommends that transmission service providers consider detailed EMT modeling when interconnecting new resources, which (at least during a transition period) may require additional time to complete during the interconnection process. Expanded studies for asynchronous resources are important to adequately assess performance of these resources and their potential impact on the BPS. NERC recommends that the Generator Interconnection Process expand the scope of its analysis regarding asynchronous resources to be more similar to analysis conducted for synchronous resources to help ensure awareness and mitigation of potential risks to reliability up front. Further, the analysis may require additional electromagnetic transient study as phase unbalances have greater impact on asynchronous IBRs than synchronous resources.

C. Distributed Energy Resources

NERC appreciates FERC's introduction of the DER (resources connected specifically to the distribution system) aggregator in FERC Order 2222 as a step toward leveraging DER capabilities to support BPS planning and operations. NERC is working with industry to evaluate the extent to which increasing participation of DERs in wholesale markets should be considered in connection with potential impacts to BPS reliability and how any reliability gaps might be mitigated. Currently, DER aggregators are not NERC Registered Entities and therefore not subject to the Reliability Standards. However, with the growing levels of DERs across North America, NERC would like to highlight that the DER aggregator will have an increasingly important and critical role to BPS reliability in the coming years as DER participation through the DER aggregator continues to grow. Accordingly, NERC will consider whether DER aggregators should be added as a NERC registered entity. The NERC SPIDERWG is also actively supporting industry in these efforts through technical reports and white papers. Coordination with state and provincial regulatory bodies will be critical, as will adoption of industry standards such as IEEE 1547-2018.

VI. Managing Cyber Risks in the Electric Power Sector

As noted in the *2021 State of Reliability Report* and the *2021 ERO Reliability Risk Priorities Report*, cyber security and physical security of the BPS remains a key focus area. NERC continues to leverage its existing tools, such as information sharing through the E-ISAC, studies and assessments, and the standards development process to evolve with these increasing risks and vulnerabilities.

A. E-ISAC Activities

Information sharing through the E-ISAC remains an effective tool in supporting industry's awareness of threats. Increased vulnerability disclosures by security and equipment vendors and

increased voluntary sharing by entities gave the E-ISAC a greater picture of the cyber security threat environment. Cyber security shares on the E-ISAC's secure portal increased by 96% in 2020 compared to 2019, leading to greater industry awareness of threats. The Cybersecurity Risk Information Sharing Program (CRISP) remains an important tool for near real-time bidirectional exchange of cyber security information. In 2020, CRISP started new pilots focused on operational technology (OT) that will increase access to data and analytic capability at the E-ISAC. The CRISP pilots further complement new work the E-ISAC is doing in 2021 to support the White House and DOE 100 Day Cybersecurity Initiative for Industrial Control Systems in the electricity subsector by increasing its visibility on these critical OT systems. Based on the effectiveness of E-ISAC programs, NERC encourages industry to increase voluntary information sharing as adversaries adopt new tactics, new vulnerabilities are exploited, and the magnitude of potential impacts change as the grid evolves and cross-sector interdependencies increase.

In 2020, as in years past, North America experienced no loss of load from reportable cyber security incidents. However, NERC has observed a step change increase in the frequency and sophistication of cyber activity. The cyber security landscape continues to evolve, guided by geopolitical events, new vulnerabilities, changes in technologies, and increasingly bold cyber criminals and hacktivists. Key threats the E-ISAC observed include supply chain compromises and ransomware attacks, in addition to malware, and phishing activity. The unprecedented COVID-19 pandemic created an increased remote cyber security attack surface for industry due to increased telework, and required greater sharing and collaboration by the E-ISAC with all levels of the electricity industry, United States and Canadian governments, and partners than ever before.

The supply chain compromise discovered in December 2020 is a prime example of the evolving sophistication of malicious activity. In this case, the widely used SolarWinds Orion

network management tool was compromised through a supply chain attack. Threat actors gained access to the SolarWinds production environment, and "pushed" malicious code to customers allowing the adversary to gain remote access. Adjacent to the SolarWinds compromise, additional research revealed the actor used its initial access to gain network privileges on the victim's system and manipulate identity and authentication mechanisms in Microsoft's 365 and Azure Cloud environments.

The E-ISAC's response to SolarWinds compromise demonstrated its ability to help members and partners mitigate potential compromises to their systems by providing timely and actionable information as well as improving collaboration/cooperation between the E-ISAC and key government partners in DOE and DHS/CISA. Using multiple toolkits, the E-ISAC analyzed information to assess the potential impacts of the attack. Subsequently, the E-ISAC worked with government and industry partners to provide support through calls and webinars summarizing the threat and mitigation actions. The E-ISAC and the Electricity Subsector Coordinating Council formed an industry Supply Chain Compromise Tiger Team of industry security professionals, which produced materials and facilitated webinars aimed at improving overall industry response. Those webinars included presentations by vendors such as Crowdstrike, FireEye, Microsoft, and SolarWinds. During this period, the E-ISAC authored 97 portal postings related to the supply chain and Microsoft Exchange compromises and held a critical broadcast program call. NERC also issued a non-public Level 2 NERC alert on December 22, 2020.

The E-ISAC shared critical information concerning other supply chain compromises. On March 2, 2021, Microsoft announced the detection of multiple zero-day exploits being used to attack on-premise versions of Microsoft Exchange Server (Exchange Online was not affected). Microsoft attributed the campaign that targeted the Exchange servers to HAFNIUM, a Chinese

state-sponsored adversary. Successful exploitation of vulnerabilities may have allowed, among other things, remote, unauthorized access and potential exfiltration of data on vulnerable Exchange servers. The immediate recommended action was to apply the patch provided by Microsoft. On March 5, 2021 NERC issued a non-public Level 1 Alert, "Microsoft Exchange On-Premise Product Vulnerability Exploitation by Advanced Persistent Threat Actor."

On July 6, 2021, staff of the E-ISAC and FERC published a joint white paper, "SolarWinds and Related Supply Chain Compromise: Lessons for the North American Electricity Industry."[22] The paper primarily focuses on the significant and ongoing cyber event related to the SolarWinds Orion platform and the related Microsoft 365/Azure Cloud compromise. It also addresses vulnerabilities in products such as Pulse Connect Secure, Microsoft's on premise Exchange servers, and F5's BIG-IP. The paper highlights the need for continued vigilance by the electricity industry related to supply chain compromises and incidents, identifies key elements of adversary tradecraft, highlights specific malwares and tools to remediate, and recommends actions to ensure the reliability and security of the BPS.

The disclosure of vulnerabilities in IT and OT supply chains continues to grow as more researchers publish results. For enterprise environments, in 2020 there was a significant increase in Microsoft vulnerabilities of 1,268 (48%) over the prior year, with reported vulnerabilities increasing 181% over the last five years.[23] OT vulnerability disclosures are also increasing with firms like Dragos reporting 703 disclosures in 2020, an increase of 23% over the prior year,[24]

[22] See whitepaper at https://www.nerc.com/pa/CI/ESISAC/Documents/SolarWinds%20and%20Related%20Supply%20Chain%20Compromise%20White%20Paper.pdf.
[23] See https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report.
[24] See https://www.dragos.com/blog/industry-news/2020-ics-cybersecurity-year-in-review/.

and Claroty reporting 637 ICS vulnerabilities being discovered already in the first half of 2021.[25] A good example of how the E-ISAC is addressing this growing threat with industry and government was the recent Blackberry QNX real-time operating system (RTOS) vulnerability.[26] A technology used differently in many critical infrastructure sectors, an RTOS vulnerability like QNX could enable an adversary to mis-operate a critical piece of equipment, including in the electricity industry. However, working with the government and original equipment manufacturers, the E-ISAC was able to contribute electricity industry remediation context to the DHS vulnerability disclosure process, and set appropriate context for the potential risk to the BPS. Conversely, when the vulnerability was released, the E-ISAC provided additional remediation guidance and context to industry on the level of risk to utilities that practiced appropriate cyber hygiene and were compliant with NERC CIP standards through an All-Points Bulletin.

Finally, the Colonial Pipeline ransomware attack – which disrupted petroleum markets in the East for several days in May 2021 – is an ominous reminder of the potential for cascading impacts due to cross-sector interdependencies. Although the attack itself had significant impacts on a system with substantial local inventories, a similar disruption to a major natural gas pipeline where in-market inventories are much less prevalent during severe winter weather could have even greater impacts on electric generation performance. In addressing potential cross-sector threats, the E-ISAC collaborates directly with other ISACs and government partners to share threat and mitigation strategies. In the case of the Colonial Pipeline attack, the E-ISAC worked

[25] See https://claroty.com/2021/08/18/blog-latest-claroty-report-ics-vulnerabilities/.
[26] See https://us-cert.cisa.gov/ncas/alerts/aa21-229a.

directly with the Cybersecurity and Infrastructure Security Agency (CISA) to share Situation Reports on the ransomware attack for member situational awareness.

B. Studies and Assessments

NERC also continues to leverage its study and assessment capabilities to address cyber security risks. In particular, at the direction of the NERC Board of Trustees, NERC has focused its studies on low impact BES Cyber Systems and supply chain risks in response to emerging threats.

For example, in light of recent cyber security events, such as the SolarWinds supply chain compromise, and the evolving threat landscape, the NERC Board took action at its February 4, 2021, to withdraw CIP-002-6, a proposed standard that permitted some entities to become a lower impact level. Furthermore, the NERC Board of Trustees also determined additional study and data was necessary to understand the impact level of certain Control Centers. As such, the NERC Board approved resolutions for (1) NERC staff to work with industry stakeholders to further study the applicability of CIP standards to Control Centers owned by a Transmission Owner (TO) that performs the functional obligations of a TOP; and (2) NERC staff to complete a broader review of the risk of presented by various facilities that meet the criteria that define low impact cyber facilities. While the NERC Board did not have indications that the low impact BES Cyber Systems were compromised by the SolarWinds supply chain compromise, the NERC Board determined to proactively evaluate and whether low impact BES Cyber Systems were protected commensurate with the risked posed by compromise of these systems, and what actions should be taken.

This reflects NERC and its Board of trustees recognition that the Solarwinds compromise substantially changed the framework related to a "coordinated attack" and recognized that supply

chain attack effectively solves the "one to one" problem with a "one to many" solution — corruption of a commonly used tool could be used to infect multiple users of that tool as opposed to attacking specific individual assets.

To carry out the first resolution, NERC and industry are working to initiate a field test under the NERC Rules of Procedure, Appendix 3A Section 6, as part of standards development Project 2021-03 CIP-002 Transmission Owner Control Centers. To carry out the second resolution, NERC assembled a team to review the risk posed by low impact BES Cyber Systems. This team is currently working on a whitepaper. As demonstrated by the Board directives and subsequent actions, the NERC Board proactively addresses risks in a timely matter, and NERC staff and industry use appropriate tools to accomplish the directives.

NERC also conducted a study in response to a directive from FERC in Order No. 843 on low impact BES Cyber Systems electronic access controls. NERC and the Regional Entities conducted a study of approximately 200 registered entities with assets containing low impact BES Cyber Systems regarding: (1) what electronic access controls entities chose to implement and under what circumstances at these assets; (2) whether the electronic access controls adopted by entities provide adequate security; and (3) other relevant information found by the ERO Enterprise as a result of the study. NERC filed a report on this study with FERC on June 30, concluding that the studied registered entities generally provided adequate security under Reliability Standard CIP-003-8 and identifying some opportunities for improvement where additional or improved controls would enhance their security posture, such as improved controls for vendor remote access.

Regarding supply chain risks, NERC has been carrying out its plan to study the effectiveness of the supply chain standards, as directed by the NERC Board of Trustees at its August 10, 2017 meeting. The plan includes the following actions:

- Conduct surveys to examine for trends on supply chain awareness, compiling statistics on identified key risk indicators, such as software validation discrepancies, information on vendors that support supply chain frameworks, entities who performed vendor risk assessments in the prior 24 months, and analysis of vendor vulnerability and cyber security incident notifications.

- Compare contractual language (pre and post Supply Chain Standards implementation) voluntarily from entities, including those who are not subject to the Supply Chain Standards, to determine whether entities have been able to successfully negotiate contracts that include required supply chain controls, or whether other controls have been required to manage the risk.

- Compile audit and compliance information on the Supply Chain Standards to determine whether the language is clear, whether entities understand what is expected, and whether there are any reliability gaps in the standards.

- Analyze supply chain communications, education, outreach, and training to determine whether vulnerabilities have been identified and successfully communicated.

C. Critical Infrastructure Protection Standards

Finally, NERC continues to improve upon its Reliability Standards through development projects focused on cyber security. As discussed previously, Project 2021-03 CIP-002 Transmission Owner Control Centers is pursuing a proposed field test, with the goal of revising CIP-002 based on the results of any field test conducted. This project seeks to accurately define medium and low transmission Control Centers to protect them commensurate with risk. Project 2016-02 CIP Modifications focuses on revisions to the suite of CIP standards to accommodate use of virtualized technologies. Project 2020-03 Supply Chain Low Impact Revisions is addressing the NERC Board directive to add requirements for entities with low impact BES Cyber Systems to (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary. Finally, NERC also continues to address the FERC directive to revise CIP-012 to address availability in Project 2020-04 Modifications to CIP-

012. Each of these efforts demonstrates NERC's continued commitment to improve its cyber security standards, while gathering information through studies to inform development.

Given the SolarWinds compromise, a new single-attack vector that would effectively mimic a coordinated attack raises significant concerns about protection of any and all externally routable devices regardless of their individual scale or impact. As discussed above, this suggests a review and potential modification of the CIP standard's bright-line criteria between high, medium, or low impact assets should be initiated.

VII. Conclusion

NERC appreciates the opportunity to participate in today's technical conference. This annual event is an important convening of reliability stakeholders to address the most salient issues, specifically the myriad challenges of a rapidly changing resource mix, the effects of extreme weather which frequently exacerbate these challenges, and the complexities of managing cyber risks. *2021 State of Reliability* demonstrates that the BPS is resilient and highly reliable, with numerous trends showing improved performance year-over-year. At the same time, the ongoing grid transformation presents many new risks that must be continually identified and addressed with appropriate measures. Ever-evolving security threats are increasing in frequency and sophistication, requiring defense-in-depth strategies. Working with FERC, industry, policymakers, and all stakeholders that collectively comprise the reliability ecosystem, NERC will continue to advance its critical mission, serving the needs of nearly 400 million people of North America who depend upon a reliable, resilient, and secure BPS.