

# 2019 Reliability Technical Conference

## Federal Energy Regulatory Commission

Remarks of James B. Robb, President and Chief Executive Officer;  
and Mark Lauby, Senior Vice President and Chief Reliability Officer

June 27, 2019

### Introduction

Thank you for bringing the reliability community together each year to review the reliable performance of the bulk power system (BPS), key challenges, and opportunities. The North American Electric Reliability Corporation (NERC) and the Regional Entities (collectively, the ERO Enterprise) were born out of recognition that reliability is a community effort requiring collective commitment by industry, policymakers, and numerous other stakeholders. Our mission to assure the effective and efficient reduction of risk to the reliability and security of the BPS has never been more important as the grid grows in complexity and security challenges remain ever present and always evolving. The Federal Energy Regulatory Commission (FERC), NERC, the Regional Entities, and industry should take pride in recognizing that BPS reliability and security is strong and continues to improve. Year-over-year performance measures show generally positive trends. This is all the more remarkable considering that the electricity sector is undergoing a rapid transformation in technology and fuel mix, with more digitized and distributed resources serving load, and persistent security threats from determined adversaries. With appropriate insight, careful planning, and continued support, we have high confidence the electricity sector will continue to navigate challenges while maintaining reliability and security.

The ERO Enterprise's core mission requires a keen focus on addressing both known and emerging risks. Priority areas include the smooth transition of the Western Reliability Coordinator function, the implications of the changing resource mix and the pace of that transformation, including inverter issues and the growing, and increasingly critical, interdependency between the electricity and natural gas industries. Security is also a priority, including the performance of NERC's Electricity Information Sharing and Analysis Center (E-ISAC) and implementation of its strategic plan, the evolution of the critical infrastructure protection (CIP) standards, as well as assessing the best way to address supply chain risk and electromagnetic pulse (EMP). NERC continues to make progress on increased effectiveness and efficiency, including the Standards Efficiency Review, the new Align compliance tool, and improvements to our committee structures. With the consolidation of two Regional Entities and new leadership in three others, the ERO Enterprise is undergoing a transformation of its own. These changes will enhance effectiveness and promote further efficiency and consistency.

### State of Reliability

The *2019 State of Reliability* (SOR) report is NERC's independent historical assessment that focuses on BPS performance during the past year as measured by a predetermined set of reliability indicators. This annual report informs regulators, policymakers, and industry leaders of reliability and performance trends, needed actions to address risks, and whether mitigations are leading to positive improvements on the system or whether additional or different interventions are necessary.

Significant and rapid changes in the electricity industry present new challenges and opportunities for reliability. The performance measures discussed in the SOR show generally positive trends in terms of generation, transmission, severe weather resilience, and protection and control performance. However, as reserve margins continue to tighten in certain assessment areas, as seen in the Electric Reliability Council of Texas (ERCOT) last year and continuing into 2019, natural gas interdependency in areas like New England and California, maintaining reliability through the resource mix transition and resulting constraints is the most significant challenge facing the industry in the coming years.

The SOR identifies the following key findings:

**Extreme weather events continue to be leading contributors to transmission, generation, and load loss.**

While extreme weather events continue to stress transmission, generation, and distribution systems, BPS reliability was maintained, and the total number of load loss events was less than the prior four years. Further, resilience to extreme weather was evidenced by good generator and transmission performance compared to the benchmark performance levels experienced during the 2014 Polar Vortex. Transmission recovery during the extreme weather events in 2018 was evidenced by quick restoration times and statistically significant reductions in transmission outage severity.

**There were no non-weather-related category 3, 4, or 5 events in 2018.**

2018 was a year of high reliability with no non-weather-related Category 3, 4, or 5 events and only one Energy Emergency Alert–Level 3 that led to firm load shedding (675 MW of load loss consisting of under-frequency load shedding (UFLS) activation, manual firm load shedding action, and interruptible load curtailment actions in Nova Scotia on November 29, 2018, lasting more than seven hours due to extreme weather). Firm load was served 99.92% of time. This does not include inconsequential load loss or load loss due to distribution outages. There were two weather-related Category 3 events: Hurricane Michael and Hurricane Florence.

**In Texas, there is projected capacity deficit in 2019, but better than expected performance from the generation fleet helped meet 2018 summer peak demand.**

Texas continues to have insufficient resources to meet the Reference Margin Level, but still successfully met demand throughout the 2018 summer season. Despite having set a new system-wide peak demand record of 73,308 MW on July 19, 2018 (which is higher than average performance from both wind and conventional generation), firm load shedding was not needed. As noted in NERC's Summer Reliability Assessment, we remain concerned about ERCOT resource adequacy as we enter the summer of 2019, but must acknowledge that the actions of ERCOT and performance of ERCOT-based generation in the past would indicate they have the tools needed to navigate this upcoming season.

**Despite continually evolving threats, no cyber or physical security incidents leading to unauthorized control actions or loss of load occurred in 2018.**

In 2018, there were no reported cyber or physical security incidents that resulted in an unauthorized control action or loss of load. Both mandatory and voluntary information sharing indicate that distribution-level events are more frequent than those affecting Bulk Electric System (BES) equipment.

While there were no NERC-reportable cyber security incidents during 2018, this does not necessarily suggest that the risk of a cyber security incident is low.

While we tout the “no load loss” statistic confidently, no one should assume any degree of complacency when it comes to grid security, either by the ERO Enterprise or industry. We observe a high level of collaboration among industry leadership through the Electricity Subsector Coordinating Council (ESCC) and evolving partnerships between industry, the E-ISAC, and the U.S. Departments of Energy (DOE) and Homeland Security (DHS) that give us confidence that industry takes the threat seriously and is initiating action to continue to buttress its defenses. That is evident through industry support of an aggressive investment in E-ISAC capabilities as well as other ESCC initiatives. Nonetheless, grid security (particularly cyber security) is an area where NERC and industry must continually improve defenses as threats rapidly evolve. Cyber threats are becoming more sophisticated so we must be vigilant.

**Misoperations continue to be reduced.**

Protection system misoperations exacerbate the severity of transmission outages. While the overall misoperations rate is slightly higher in 2018 than 2017 (8.6%, up from 7.1% in 2017), a statistically significant downward (positive) trend is shown over the past five-year period. The three largest causes of misoperations in 2018 were the same as in 2017: Incorrect Settings/Logic/Design Errors, Relay Failure/Malfunctions, and Communication Failures.

**There were frequency response improvements in all Interconnections.**

Frequency response arrests and stabilizes frequency during system disturbances. NERC closely monitors the frequency response of each of the four Interconnections and measures the margin at which UFLS would be activated. UFLS provides a vital safety net for preserving Interconnection reliability, and measuring the margin allows NERC and industry to ensure there is adequate frequency response on the system. For all Interconnections, frequency response performance improved in the arresting and/or settling periods. Specifically, the Eastern Interconnection, the Texas Interconnection, and the Québec Interconnection showed statistically significant improvements in the arresting period from 2014 through 2018. The Texas Interconnection, Québec Interconnection, and the Western Interconnection exhibited statistically significant improvements during the stabilizing period from 2014 through 2018.

**As more inverter-based generation is added, solutions to emerging reliability challenges are being identified.**

Inverter-based generation includes solar photovoltaic (PV) and many forms of wind generation. A number of routine transmission line outages have led to the unplanned and wide-spread loss of significant amounts of predominately BPS-connected, inverter-based generation. In 2017, the Inverter-Based Resource Performance Task Force was established to study the issue and inform industry on the risks posed and options for mitigating them. In 2018, industry began implementation of the Inverter-Based Resource Performance Guideline. This, along with wide-spread recognition of the challenge, has gathered the industry’s best technical experts to develop solutions through a variety of new protection and control requirements, clarification to NERC Reliability Standards, and technical specifications through the Institute of Electrical and Electronics Engineers (IEEE). In addition to the excellent technical work being

accomplished by the ERO Enterprise, industry, and the supply chain of solar developers and inverter manufacturers, this is an outstanding example of how to approach complex issues and solve important reliability and security issues through collaboration across the industry.

### **Reliability Risk Priorities Report**

Whereas the SOR is a near-term assessment reviewing historical performance, NERC's *Long-Term Reliability Assessment* serves as a comprehensive, reliability-focused perspective on the 10-year outlook for the North American BPS. Together, these two reports provide NERC's Reliability Issues Steering Committee (RISC) with information regarding emerging risks. The RISC is an advisory committee comprised of senior industry leaders that reports directly to NERC's Board of Trustees to help prioritize BPS reliability risks of strategic importance. Its members include leadership from the NERC Member Representatives Committee, at-large members, as well as the NERC standing committee leadership. The RISC leverages stakeholder expertise to produce the ERO Reliability Risk Priorities Report (RISC Report), which complements the SOR. Namely, it takes a longer-term view of potential risks and identifies potential mitigations to ensure that the system is prepared for emerging risks. This report is produced biennially to inform industry, regulators, and policymakers about critical risks to the BPS and viable approaches for mitigating those risks.

The RISC Report is the culmination of extensive collaboration between NERC, the RISC and industry. In March, the RISC held the Reliability Leadership Summit where industry and policy leaders convened for a day-long engagement to capture and refine key risk elements. Along with input from the Summit, the RISC identified potential mitigating activities that would lower the overall risks and their impacts to grid reliability. A survey was distributed to industry executives to rank the risks in order of their impact to grid reliability and to assess the effectiveness of potential mitigation activities. NERC documented the findings from 150 diverse survey responses along with the work of the RISC.

The 2019 RISC Report – expected to be published in August – will identify the following risks for more industry collaboration and concerted efforts to develop industry solutions: physical security vulnerabilities, cyber security risk, critical infrastructure interdependency, changing resource mix, BPS planning, and resource adequacy and performance. While some risks have been previously identified by the RISC and are presently being addressed by industry, other newer, emerging risks require more assessment by industry, regulators, and policymakers in order to effectively mitigate these risks.

### **Identifying and Addressing BPS Risk**

The ERO Enterprise uses BES performance data, event analysis information, compliance monitoring, and other means to effectively identify and prioritize risk to the BPS. These tools help inform mitigations to address risk through updates to Reliability Standards, or through other reliability improving measures.

In addition to traditional reliability assessments, the ERO Enterprise produces detailed assessments of emerging risks which provide crucial data on characteristics associated with the changing electric industry. For example, in 2014, the polar vortex tested the resilience of the North American BPS. This event served as an example of how extended periods of cold temperatures have direct impacts on generator resource availability. Higher than expected forced outages were observed during the 2014 Polar Vortex

(particularly for natural-gas-fired generators) as well as higher-than forecast peak demand. An analysis of the Generator Availability Data System (GADS) following this event highlighted the interdependencies of gas and electricity. Since then, there have been significant efforts to improve generator performance during severe cold weather, and marked improvements in forced outage rates have been observed during subsequent winter periods.

That said, there were two occurrences, one in 2018 and another in 2019, where local issues were experienced during cold weather with generating units experiencing higher outage rates than average performance. While not a categorized event in 2018, the operating condition led to the system being postured in a certain way that had the potential to cause an adverse reliability impact to the BPS. As a result, a joint NERC-FERC inquiry was conducted. At this writing, the joint report has not yet been released. These events understandably raise the question of whether more prescriptive requirements around cold weather coordination, planning, fuel assurance and preparation are desirable.

Tools like Situation Awareness for FERC, NERC, and Regional Entities (SAFNR) help ensure that the ERO Enterprise is aware of the real-time status and any pressing needs of the BPS. SAFNR data provides NERC with near real-time information about the BPS. This allows NERC to coordinate in near real-time with critical infrastructure operators, federal, and local agencies and authorities during an event or severe weather. NERC, with support from the Regional Entities, is enhancing the SAFNR tool to include features such as geospatial views of the BPS.

NERC is also improving the content of its databases. To keep pace with the changing resource mix, NERC needs data from all types of generating resources that may have an impact on reliability. GADS performance data now captures wind generation. NERC has developed wind turbine generation data reporting instructions to assist wind plant personnel in reporting information to the GADS application. Wind plants with a total installed capacity of 75 MW or more with a commissioning date of January 1, 2005 or later will be required to report their performance on a quarterly basis according to a set schedule. NERC is leveraging its technical standing committees to determine appropriate data reporting requirements for solar data reporting, with the goal of preparing a Section 1600 data request.

The ERO Enterprise uses its analytical capabilities to identify previously unknown risks to reliability. These capabilities inform new or updated Reliability Standards, and other effective strategies. For example, inverter-based resource controls, protection, and performance issues were brought to the forefront by NERC efforts. Following analyses of the Blue Cut and Canyon 2 fires, NERC posted alerts in 2017 and 2018 to address this issue and formed a joint Inverter-Based Resource Performance Task Force to develop guidelines and recommended practices for inverter-based resources connected to the BPS. This work has also led to proposed enhancements to PRC-024-2 – Generator Frequency and Voltage Relay Settings. The proposed changes identify a number of technical issues that require clarification and correction to ensure inverter-based generator owners, operators, developers, and equipment manufacturers clearly understand the intent of the standard so their plants respond to grid disturbances in a manner that contributes to the reliable operation of the BPS. This example reflects the steps that NERC and the ERO Enterprise, working collaboratively with industry, has taken to better understand the changing resource

mix, identify mitigation solutions, monitor their implementation and, thereby, improve reliability of the BPS as the grid evolves.

There are other examples of data and analysis used to support new and updated Reliability Standards:

- Proposed Reliability Standard TPL-001-5 was developed following an assessment of single points of failure on protection systems using data collected pursuant to the ERO Enterprise's authority under Section 1600 of the Rules of Procedure (ROP). The analysis of this data, which was prepared by two technical subcommittees with the assistance of NERC staff, helped identify the extent of the reliability issue and informed the development of the proposed standard.
- The ERO Enterprise has executed its responsibilities for Reliability Standard BAL-003-1.1 (Frequency Response and Frequency Bias Setting) using expertise from Reliability Assessments, Reliability Standards, and Compliance, with support from the Operating Committee and its Resource Subcommittee. In the course of implementing the standard, NERC identified issues that led to a two-phase standard authorization request (SAR): first, to correct the standard, and second, to improve the operation of the standard. NERC plans to present reliability Standard BAL-003-2 to the NERC Board in 2019 and to continue work on future BAL-003-3 in 2020.
- Using the latest in scientific and technical understanding, NERC developed two Reliability Standards addressing potential geomagnetic disturbance (GMD) events: Reliability Standard EOP-010-1 (Geomagnetic Disturbance Operations) and three versions of the TPL-007 Reliability Standard (Transmission System Planned Performance for Geomagnetic Disturbance Events). Further, NERC began work on a FERC mandatory request for GMD data pursuant to Section 1600 of the NERC ROP to improve the availability of GMD data.
- In 2018-2019, at the direction of the NERC Board, NERC staff prepared a report on cyber security supply chain risks with recommendations for future actions. NERC staff worked with the Electric Power Research Institute (EPRI) to provide an independent assessment of industry supply chain risks and presented an interim report to the NERC Board in August 2018. The final report was presented to the NERC Board in May 2019. Recognizing the complex and evolving nature of supply chain risks, this final report contains several recommendations for further study (including the study of data collected pursuant to a forthcoming ROP Section 1600 data request) and Reliability Standards development work.

While Reliability Standards play an integral role in helping to assure the reliability of the BPS, NERC has other tools available to help address new and emerging risks. For example, NERC's Planning Committee has formed the Electric Gas Working Group, which is in the process of developing an industry guideline on fuel assurance. This guideline will help address natural gas pipeline contingency risk to BPS reliability. The working group has been charged with completing this industry guideline by yearend. The guideline will include suggested parameters for studying these high impact, low frequency events as well as establishing guidance for contingency planning and assuring system resilience. NERC recognizes the increasing trend toward more gas-fired electric generation along with the differences in delivery of natural gas vs. other fuel types. Additionally, weather phenomena such as the polar vortex and bomb cyclone events put

additional pressure on the natural gas pipeline system and reliable deliveries. These cold weather events along with limited, dual-fuel capability, a lack of firm transportation for many generators, uncertainties with natural gas storage, and the potential for severe outages as a result of a major pipeline rupture call for industry guidance. Once implemented, the effectiveness of the guideline will be monitored and evaluated to determine whether a standard is needed on pipeline and other fuel contingencies.

NERC continues to work collaboratively with those who share our reliability and security mission. This includes reinvigorating our relationships with a number of organizations. For example, NERC and the North American Transmission Forum recently renewed our memorandum of understanding toward sharing of information and activities toward complementing our abilities to identify and mitigate risks to reliability. Additionally, NERC and the North American Energy Standards Board continue to work together to support the effective and efficient use of standards for reliability and business practices. Finally, NERC continues to support the North American Generator Forum and work closely with EPRI.

EPRI recently completed a three-year research project identifying potential impacts of EMP on the electric transmission system. This report provides the technical groundwork for mitigation actions. Based on EPRI's results, NERC has launched a task force to identify next steps and actions to address EMP reliability concerns. The task force will review EPRI's work in detail, identify key areas of concern and improvement, submit any needed best practices and reliability guidelines, and develop, if needed, any SARs. During the third quarter of 2019, the task force intends to publish draft recommendations and any guidelines and recommendations. By the end of 2019, the task force will present SAR(s) to the Standards Committee, if applicable.

### **Addressing Cyber and Physical Security – Continued Engagement**

The security landscape is dynamic, requiring constant vigilance and the agility to respond to new and rapidly changing events. NERC's mandatory CIP standards are a foundation for security practices. They provide universal, baseline protections and are unique among critical infrastructure industries. Due to the ever-evolving nature of cyber threats, quick, accurate and secure communication is a key defense. Accordingly, NERC's E-ISAC serves as the information sharing conduit both within the North American electricity industry and between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to determine and maintain "ground truth" during rapidly evolving security events through analysis, communication and coordination among the North American electricity industry.

The E-ISAC also plays a key role in cross-sector coordination, focusing on sectors with which electricity has interdependencies, such as natural gas, water, and other critical infrastructure. The E-ISAC works closely with DOE, DHS, FERC, and the ESCC as well as our security partners in Canada to further the public-private partnership so important to addressing security. In addition, every two years, NERC sponsors GridEx, a continent-wide exercise that looks at how industry and government manage a coordinated cyber and physical attack on geographically distributed targets. The exercise involves a day of "distributed play" followed by an executive tabletop where industry, NERC, and government representatives discuss how best to address identified needs and risks. A public report is issued and the ESCC is tasked with follow up on these matters.

## **E-ISAC Long-Term Strategic Plan**

The E-ISAC's mission is to reduce cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. It accomplishes this mission by sharing trusted information and analysis in a timely, credible, and actionable manner with asset owners and operators across the continent. The E-ISAC is currently in the second year of its five-year long-term strategic plan, driven by three important considerations: security threats continue to evolve and become more dangerous, member expectations for highly reliable energy continue to increase, and industry needs a more robust understanding and measurement of grid resiliency and security. To address these considerations, the E-ISAC strategic plan is focused on activities that improve information collection, analysis, and dissemination of actionable intelligence.

To meet the E-ISAC's mission and assist industry with its preparation and response to cyber and physical threats, the E-ISAC uses a secure portal as the primary means for communicating with electricity industry member organizations. The E-ISAC receives, as well as dispatches, security information related to the grid. The portal was revamped in 2017 and upgrades are regularly implemented to enhance the user experience. The new portal functions, plus greater outreach with key industry stakeholder groups through our Industry Engagement Program, have improved bi-directional information sharing and allows members greater access to more information. We currently have about 7,000 portal users (E-ISAC membership is not limited to registered entities and extends to all electric system asset owners and operators).

In addition to the secure portal, the E-ISAC shares information through several forums to increase awareness of threats and to recommend mitigations. When a significant security concern arises, NERC and the E-ISAC can provide content to NERC alerts to provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. In addition to NERC alerts, the E-ISAC uses the Critical Broadcast Program (CBP), which was launched in 2018 to rapidly share information with members. The CBP leverages E-ISAC staff and stakeholder expertise to obtain and share the best available information and potential mitigation strategies to address developing security threats and events in a timely manner, either through conference calls or threat and mitigation bulletins. We have recently upgraded the capacity and processes for organizing and executing a CBP call to allow for multi-sector participation as appropriate. In 2019, we implemented an "All Points Bulletin" to immediately alert industry and direct them to the portal of security issues which are time sensitive yet may not warrant a CBP call. Further, the E-ISAC hosts regular monthly threat briefings, unclassified threat workshops, participates in classified forums with its members, and allows asset owners and operators to interact with our analysts and each other to share trend analysis and context on common threats to the electricity industry.

The Cybersecurity Risk Information Sharing Program (CRISP) is managed by the E-ISAC and in partnership with DOE. CRISP uses innovative technology and leverages DOE and its National Laboratory System's analytical capability. CRISP provides timely two-way sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. CRISP companies cover more than 75 percent of U.S. customers. CRISP information is shared in a secure fashion through the E-ISAC portal,



and allows non-CRISP member companies to benefit from the shared indicators and threat actor activity captured by the program.

CRISP information also supports the development of situational awareness to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources. In addition to CRISP, the E-ISAC is pursuing cyber-automated information sharing systems as well as a malware analysis repository and threat information exchange to provide for more advanced information sharing capabilities. Complementing the automated systems, the E-ISAC continues to increase collaboration with the Intelligence Community outside of CRISP to improve the flow of information. NERC is working with DOE to expand participation in CRISP to smaller entities. In addition we are exploring options to expand the CRISP data set through partnerships with other entities and vendors (e.g., Canadian entities through the Independent Electricity System Operator in Ontario and smaller public power entities).

E-ISAC services enable industry to respond to and defend against cyber and physical security threats, vulnerabilities, and incidents through the exchange of timely, actionable information. In particular, to further enhance cross-sector collaboration in light of electric and natural gas interdependencies, the E-ISAC continues to expand its partnership with the Downstream Natural Gas ISAC (DNG-ISAC). In the past year, the E-ISAC added additional partnerships with other interdependent sectors, including the Water-ISAC and the Multi-State-ISAC with the goal providing electricity industry context to water and wastewater operators, as well as state and local government, and, in turn, enhancing context for the electricity sector. The E-ISAC is also participating with the Financial Services-ISAC on its Financial Systemic Analysis & Resilience Center (F-SARC) pilot.

The E-ISAC continues to explore partnerships with the U.S. and Canadian governments, as well as research universities and respected operational technology cyber security vendors through the DOE-funded *Neighborhood Keeper* project. We are in conversations with DOE and their Cyber Analysis Tools and Techniques (CATT) 2.0 initiative to create a multi-sector data lake of information technology and operational technology data.

As FERC considers activities to support the E-ISAC's mission, it is important to stress the role of partnerships and robust voluntary information sharing. These partnerships include the Office of Energy Infrastructure Security's efforts with industry to develop high-level, anonymized trends to help inform decisions and investment in cyber security infrastructure by asset owners and operators. Additionally, FERC may consider further encouragement of state and local governments to protect and anonymize that information, which may increase the additional voluntary information sharing needed to protect the electricity industry.

### **ERO Enterprise Transformation**

Another issue of note is the transformation of the ERO Enterprise itself. The combinations of the Midwest Reliability Organization and the former Southwest Power Pool-Regional Entity, and the prospective combination of SERC and the Florida Reliability Coordinating Council Regional Entity will streamline the

structure of the ERO Enterprise from eight diverse Regions to six Regions of more comparable size and complexity.

Importantly, we have restructured the leadership of the ERO Enterprise into a unified Executive Committee consisting of the CEOs of the Regional Entities and the senior officers of NERC. This group is committed to working together to advance reliability and security across North America. The group is focused on assuring we bring best talent to bear to solve complex problems, evolve our tool set to be relevant to the challenges industry faces today, and innovate our approaches accordingly, while still balancing our unique ability to collaborate with industry with our need for independence to call issues as we see them. It is a powerful model and one we are proud to steward on behalf of the nearly 400 million citizens in North America who rely on us to assure the reliability and security of the BPS. Electricity is a critical part of the fabric of modern society. While NERC and the Regional Entities don't own or operate any assets, we play a key role in assuring society of a reliable and secure BPS.

### **Conclusion**

The ERO Enterprise is fulfilling its critical mission dedicated to reliability and security of the BPS. The BPS continues to perform reliably and in a secure manner, with generally positive trend lines over time. While these significant achievements should be well-recognized, adaptation to a rapidly changing grid with the associated evolving risks remains the preeminent challenge. Future success is measured by our continued ability to anticipate, identify, and address evolving risks. Accordingly, the ERO Enterprise remains keenly focused on ensuring that our programs evolve with the challenges so they are fully aligned with the changing reliability ecosystem. Reliability and security is a community effort. With an acute focus on risk, careful planning, and continued commitment from industry, regulators, and all stakeholders, the electricity sector will continue to navigate challenges successfully.