NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Long-Term Strategy

November 2017

Introduction

As the ERO Enterprise[1], our vision is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure effective and efficient reduction of risks to the reliability and security of the BPS.

This *ERO Enterprise Long-Term Strategy* (Long-Term Strategy) looks ahead five to seven years to examine how changes in the industry and reliability ecosystem will affect how we achieve our vision and mission in the future. We anticipate significant changes in resource mix, a proliferation of fast-acting digital protection and control technologies, and increased integration of distributed energy resources. We also anticipate cyber security and resilience from natural as well as manmade events will become more central factors in a reliable BPS. These changes will introduce new players into the reliability arena, alter how we define and measure reliability, and affect how risks are managed. Cyber security and the expansion of distributed energy resources will also create jurisdictional challenges as the line between distribution and bulk power blurs and events on the distribution system can have significant impacts on the BPS. This Long-Term Strategy outlines the driving forces behind the changing reliability ecosystem and presents six strategic focus areas to ensure the ERO Enterprise preserves its current strengths and achievements in assuring BPS reliability, while adapting to the significant changes ahead of us.

Background and Purpose

Over the past five years, NERC and the Regional Entities have made progress in strategic planning and operational coordination, including the development of a three-year *ERO Enterprise Operating Plan* (Operating Plan) to guide coordinated operations and annual resource budgeting. The Operating Plan includes a set of operational goals and general description of the contributing activities that will be undertaken by NERC and the Regional Entities over a three-year period. Further details, resources, and resource allocation in support of these goals and contributing activities will be set in the NERC and Regional Entities' annual business plans and budgets. Metrics and supporting measures accompany the Operating Plan and will be reviewed and updated as needed on an annual basis.

In November 2016, the NERC Board of Trustees (NERC Board) accepted the Reliability Issues Steering Committee's (RISC's) report regarding reliability risk priorities[2]. The RISC report includes risk profiles and recommendations that reflect discussions with technical committees, industry dialogue through a series of executive leadership interviews, and technical reports, assessments, and analysis provided by NERC and the Regional Entities. In March 2017, the RISC continued its work by sponsoring a Reliability Leadership Summit (Summit) in the form of a series of executive level panel discussions to identify the most significant existing

[1] The ERO Enterprise is comprised of NERC and the eight Regional Entities, which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the ERO's statutory obligations to assure the reliability of the North American BPS.

[2] ERO Reliability Risk Priorities, RISC Recommendations to the NERC Board of Trustees, November 2016

and emerging risks to reliability. In June 2017, the Federal Energy Regulatory Commission (FERC) also held a reliability technical conference to identify reliability priorities.

Based on the latest RISC report, Summit, FERC technical conference, and additional work by the RISC and NERC to conduct pulse point interviews with industry executives[3], NERC Board members, and the ERO Enterprise officers, one concludes that the electricity industry is undergoing change at a pace never before seen. The ERO Enterprise must have a long-term strategy that recognizes these significant new developments affecting the reliability of the BPS and identifies key focus areas to guide the ERO Enterprise over a five-to-seven-year horizon.

While the ERO Enterprise has a central responsibility in identifying and addressing BPS reliability risks, ensuring BPS reliability requires a long-term collective commitment by many organizations. Industry, industry forums and associations, software and equipment vendors, research organizations, governmental authorities, and other reliability stakeholders all must play important roles. Industry has a critical role as planners and operators of the BPS as well as in providing hands-on expertise that informs and supports ERO Enterprise decision making, activities, and priorities. FERC and the Department of Energy (DOE), Canadian and Mexican regulators, federal, state, and provincial policymakers also have significant responsibilities in providing oversight and developing and implementing policies to foster and protect BPS reliability and resilience.

Emerging Risks and Challenges

The following is a summary of the major emerging risks and challenges that were identified in evaluating trends and future scenarios.

Impact of Policies, Regulations, and Changing Economics

Policy and regulatory developments at the federal, provincial, state, and local levels, changing economics related to fuel, and new technologies are driving changes in both the demand and use of electricity as well as the nature of risks that can affect BPS reliability and security. Examples include policies and regulations governing renewable portfolio standards, conservation, electricity storage, demand response, micro-grids, and distributed electric energy resources. These policies are typically not consistent throughout North America, complicating the ability to model and assess their potential impacts on BPS reliability and security. Further, the transition to a lower carbon system is accelerating as the cost of renewable technologies decreases along with the decline of natural gas prices. The ERO Enterprise will continuously work with policymakers to increase their understanding of electricity policy impacts on BPS reliability, as well as communicate the strength and value of North American electric reliability collaboration.

Policies and regulations also impact decision making for electricity sector acquisitions and divestitures, fuel supply, energy demand, generation, transmission, and distribution investments and operations. This further complicates the ability to model, understand, predict, and address potentially significant BPS reliability and security impacts. These changes are also occurring at a time when declining industry revenues and

[3] This includes input from the RISC, the Members Representatives Committee (MRC), NERC's Planning Committee, Operating Committee, Critical Infrastructure Protection Committee, and Compliance Certification Committee, trade associations, and industry forums.

increased customer preferences for control, sustainability, resiliency, and lower costs are complicating and, in some instances, placing pressure on investment decisions necessary to maintain reliability, security, and resiliency.

Global threats in physical and cyber security are creating new challenges for the electricity sector,[4] and both policymakers and the public are increasingly aware of and concerned about these threats. The security landscape is dynamic, requiring constant vigilance and agility. The ERO Enterprise supports grid security through a comprehensive series of strategies involving mandatory standards, information sharing, and strategic partnerships. NERC's mandatory critical infrastructure protection standards are a foundation for security practices and they provide universal baseline protections. However, due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Additional resources and capabilities are required to respond to an ever-changing threat landscape. The number of constituencies at federal, state, provincial, and local levels that are focusing on resiliency, security, and reliability is also growing. This increases the need and importance of accurate, coordinated, and timely information sharing between the electric industry and government.

Proposed increases in cross-border electricity trade and rapid expansion of interconnection ties with Mexico will require increased cooperation in evaluating and addressing reliability and security considerations. Consistency should be pursued to the extent necessary to support comparable levels of reliability, while giving deference to the authority of sovereign jurisdictions and respecting the occasional need for differing approaches based on regional or provincial technical or industry structure differences. Transparency is essential to enable the ERO Enterprise, regulators, and industry stakeholders to assess the effectiveness of standards and other programs, but transparency must be balanced with appropriate protections for confidential information.

In Canada, NERC standards are adopted as mandatory and Canadian stakeholders make significant contributions to standards, assessments, and compliance through established collaboration mechanisms. Recognizing this maturity, a continued focus on continent-wide consistency and transparency will help to further develop and enhance the value of the ERO model to reliability. Efforts with Mexico are comparatively recent. On March 8, 2017, NERC, the Comisión Reguladora de Energía, and the Centro Nacional de Control de Energía signed a memorandum of understanding (MOU) that outlines a framework for a cooperative relationship between NERC and Mexico to further enhance the reliability of the North American BPS. The ERO Enterprise will work with Mexican counterparts to develop and implement the framework outlined in the MOU with the goal of supporting Mexico in its ongoing efforts to ensure reliability as it reforms and modernizes its electric system.

Changing Reliability Ecosystem

The policies and economic factors described above are driving numerous developments in the electric generation, transmission, and distribution systems that are used to provide reliable electric service to consumers in North America. For example, large central station coal and nuclear plants are being retired

[4] Keeping America Safe; Toward More Secure Networks for Critical Sectors; Massachusetts Center for International Studies and Massachusetts Institute of Technology Policy Research Initiative. March 2017, pages 27-32.

due to market pressures and environmental regulations. Siting and constructing new transmission and central station generation infrastructure is both difficult and expensive. Electricity production in several regions is becoming more heavily dependent on the availability and security of natural-gas supplies and associated gas transportation and storage infrastructure. Increasing natural gas dependence for power production creates the potential for larger single-points-of-disruption to the electricity system where, for example, a number of generating plants may share a single pipeline, or be dependent on key gas storage facilities or compressor stations.

Further, digital control technologies with micro-second response times are being deployed with the modernization of transmission systems, wind and solar facilities, distribution systems, micro-grids, and distributed energy resources. These devices operate at speeds that are orders of magnitude faster than traditional reliability control and protection systems, and require careful integration and coordination with existing reliability controls. It remains uncertain at this time whether the increased system complexity of digitized systems will be mitigated by potential reliability gains through computer-to-computer system automation.

Many of these newer digital devices will be communicating over local and regional wireless networks that have increased cyber security risks. In addition, there is a dramatic increase in attempted cyber intrusions at all areas of the electricity system, including nation-state sponsored intrusions. Increased cyber dependence and vulnerabilities can also impact the delivery of natural gas, as well as disrupt telecommunications and water, upon which the BPS is dependent.

Customer load characteristics are also changing rapidly, with loads becoming “stiffer,” or less responsive to system conditions, as technologies (e.g., light emitting diodes [LEDs] and adjustable speed motor drives) are deployed. Behind-the-meter generation, energy conservation technologies and practices, and the economies of some regions are also significantly affecting customer usage and load profiles. The growth of large data centers and associated power supply and quality demands require increased focus on the availability, stability, and security of generation and transmission resources. Electric vehicles continue a growth trend with major vehicle manufacturers promising further expansion, and other areas of electrification will expand opportunities for electricity storage and control automation at the distribution level.

Large synchronous generators have traditionally helped to stabilize the electric grid. Many of these large baseload generating units are either being retired or will no longer be dispatched as baseload units. Distributed and inverter-based asynchronous renewable generation resources will continue to grow rapidly. This shift in resource mix and how resources are dispatched make it essential that steps are taken in this transition to ensure there will be sufficient amounts of essential reliability services (e.g., frequency response, ramping, and voltage support) are available. This is occurring at the same time that electric loads are becoming less able to respond to or tolerate changes in frequency and voltage.

The penetration of wind and solar resources connected to the grid through inverter-based technology, combined with stiffer loads, can alter power system performance. When asynchronous resources with inverter technology replace the synchronous generators that have large rotating masses, the system may

be less capable to dampen the impacts from routine system disturbances (e.g., lightning strikes), increasing the potential for instability. Namely, unless the necessary steps are taken to address system needs, the remaining synchronous resources may not be able to offset the immediate imbalance between power supply and demand during these events. While the addition of batteries and high-speed protection systems helps mitigate this risk, their incorporation increases the complexity of system control. Though there are benefits resulting from technology implementation, the added system complexity must be both understood and managed.

In addition to the increase in inverter-based asynchronous renewable generation resources, stability margins are being reduced due to increasing amounts of resources being located on the distribution system. It is challenging to plan and operate the BPS when the total amount of resources is unknown (unobservable) and not easily controllable. For example, solar resources may be significantly reduced if cloud-cover arrives, creating steep ramps that may outpace generating units' ability to increase output. The imbalance may result in firm load shed or system instability unless operator action is taken quickly.

System complexity, challenges in coordination between distribution and the BPS, and loss of operator situational awareness of locally controlled resources and load may increase human performance errors. The potential for common mode failures (e.g., loss of a major pipeline supply for generation, equipment failures from common system conditions, or concurrent cyber-attack on the electric grid) increases the potential for outages beyond current contingency planning.

The nature and pace of technology changes require increased workforce training and the development of skills in new areas. Partnerships are needed between academic institutions and industry to develop programs to educate, train, and grow a future workforce capable of addressing these challenges.

Recommended Strategic Focus Areas

As summarized above, there are significant policy and technical forces that are driving a rapid change in how electricity systems are designed, planned, operated, and secured. The new reliability ecosystem will include new risks, new complexities, new terminology, new reliability requirements, new players, and jurisdictional challenges. The ERO Enterprise must anticipate these changes and adapt in the five-to-seven-year horizon to achieve the vision of a highly reliable and secure BPS in the future. The focus areas outlined below are intended to guide operations planning, resource allocation, and annual budgeting to support the ERO Enterprise in both preserving its current progress and achievements and adapting to meet the new challenges.

The first two areas are grouped together below and are focused on the ERO Enterprise preserving and building on current achievements toward establishing risk-based controls to minimize BPS reliability risk while also driving additional enterprise-wide operational efficiencies and effectiveness. These two focus areas will continue to represent the majority of ERO Enterprise's focus and resource allocation—efficiently and effectively maintaining the foundation of the highly reliable BPS through risk-based approaches in standards, compliance, enforcement, event analysis, lessons learned, and other programs focused on conventional reliability issues. The ERO Enterprise must succeed in these areas.

The next three focus areas are also grouped together below and represent areas of emphasis where the ERO Enterprise must be capable of recognizing and adapting to change to achieve its mission in the five-to-seven-year horizon. This will require leadership, innovation, and new approaches in identifying, evaluating, and addressing issues affecting BPS reliability and security in areas that are not yet fully understood or developed. It will also require improvements in communication strategies, knowledge transfer, and engagement with stakeholders across North America.

The final focus area recognizes the increasing reliability and security interdependency among the United States, Canada, and Mexico and activities that are important to strengthening the role of the ERO throughout North America.

Build on and Preserve Current Achievements (Focus Areas 1 and 2)

Focus Area 1: Achieving and Maintaining Risk-Based Operations

The ERO Enterprise will achieve and maintain a risk-based focus in its operations, prioritizing and focusing resources on significant BPS reliability risks. This includes completion of the transition to risk-based compliance and enforcement with a focus on an entity's inherent risk, internal controls, and its history of significant violations. The ERO Enterprise will be effective in using compliance and enforcement to promote improved reliability and security controls in industry and reducing the number and severity of system events. For example, compliance auditors will be capable of evaluating a registered entity's risk and conducting thorough and helpful internal control reviews. The ERO Enterprise will review and approve mitigation activities that reduce risks to reliability associated with cyber and physical security as well as planning and operations. The ERO Enterprise will work with industry and other stakeholders to review and streamline standards, compliance, and enforcement activities to (1) reduce program inefficiencies and (2) assist registered entities in understanding both the necessary steps to achieve compliance with applicable standards and the benefit of integrating compliance into their internal and operating controls environment.

The ERO Enterprise will also work closely with industry, industry forums, and other organizations focused on BPS reliability to perform ongoing analysis of significant known reliability risks (e.g., vegetation management, protection system misoperations, human error, and system stability), and develop recommendations on how to best address any such risks, whether through standards or other programs and methods. Through deployment of new tools, the ERO Enterprise will significantly expand risk information sharing and analysis among NERC and Regional Entity functional areas and with registered entities. Programs will promote risk-based continuous learning and improvement that help industry avoid large events (e.g., event analysis, human performance education, lessons learned, and feedback loops). Examples of tools with potential growing importance may include broader communications of lessons learned with follow-up evaluation of effectiveness.

Focus Area 2: Being More Effective and Efficient

Economic pressures facing industry and consumers, coupled with increased enterprise resource demands, make it critical that the ERO Enterprise identify and implement mechanisms to achieve

greater enterprise-wide effectiveness, efficiency, and cost savings. Improvements in efficiency are essential to mitigating the ongoing cost of maintaining and improving the quality and effectiveness of ERO Enterprise operations, and to offset emerging focus areas as outlined in this strategy paper.

The ERO Enterprise must establish procedures to routinely and systematically review major processes with the objective of identifying and implementing efficiency improvements. The ERO Enterprise will utilize technology to improve efficiency and reduce costs as well as ensure that process improvements and organizational efficiencies associated with current and planned ERO Enterprise technology investments are realized.

It is also essential that the ERO Enterprise be engaged with industry leadership to ensure the productive, efficient, and effective engagement of industry technical expertise, which is so critical to the success of the ERO Enterprise's mission.

NERC management will work with the NERC Board to evaluate opportunities to improve the efficiency and cost effectiveness of in-person NERC Board and NERC Board committee meetings. Management will also work with the Board, MRC, the leadership of NERC standing committees, and other stakeholders to improve the efficiency, effectiveness, and value of the MRC, standing committees, task forces, and working groups. Similar initiatives will be undertaken at each of the Regional Entities. New models of engagement will be explored to determine how best to bring executive leadership into the strategic direction of the ERO Enterprise while engaging more agile groups with the best expertise available from industry and elsewhere.

The ERO Enterprise will also work with the transmission and generator forums, trade associations, and other organizations to identify specific areas where these organizations may be capable of assuming a greater role in identifying and assisting industry in mitigating reliability risks.

Adapt to Change (Focus Areas 3–5)

Focus Area 3: Identifying and Assessing Emerging Risks

In addition to the preparation of traditional reliability assessments such as the annual Long-Term Reliability Assessment, the ERO Enterprise will prepare detailed assessments of emerging risks based upon specific circumstances and available data. The evaluation of early indicators of risk can be made a more compelling cause for action when supported by the appropriate data and analysis. As an example, a detailed analysis of the Aliso Canyon experience[5] will drive specific actions to further support BPS reliability that would not be apparent through a more generalized description of gas dependency concerns. The Blue Cut fire report on solar inverter issues[6] is another specific example of a latent risk being identified and addressed early. To effectively support policies and activities necessary to ensure BPS reliability, the ERO Enterprise will prepare assessments of new BPS risks based upon case specific examples of real and potential impacts associated with the

[5] Short-Term Special Assessment: Operational Risk Assessment with High Penetration of Natural Gas-Fired Generation, May 2016
[6] 1,200 MW Fault Induced Solar Photovoltaic Resource Interruption Disturbance Report, Southern California 8/16/2016 Event, June 2017

changing resource mix, renewables, distributed energy resources, digital controls, fuel dependencies, cyber security, and other emerging challenges. Some of these assessments may focus on risks in the distribution system that may cascade into the BPS.

The ERO Enterprise will engage industry stakeholders and policymakers on reliability attributes essential to support the long-term reliability of the BPS, including equipment controls that enable system support from variable energy resources, improved visualization of dynamic/transient and voltage risks to the BPS, and accommodating distributed energy resources such as small end-use customer resources. The ERO Enterprise will encourage vendors of power system simulation software to develop programs to enhance dynamic load modeling capabilities.

Working closely with NERC's Planning and Operating Committees and other stakeholders, the ERO Enterprise will (1) expand and improve data gathering, validation, modeling, and analysis to identify and assess the BPS reliability impacts of new and emerging risks and (2) determine if modifications to Reliability Standards are necessary to address emerging risks, including impacts associated with essential reliability services. The ERO Enterprise will collaborate with BPS planning coordinators to assess the reliability impacts associated with fuel delivery and storage and on how to assess these impacts in the context of long-term planning studies.

The ERO Enterprise will support the development of new planning tools necessary to enable timely, probabilistic assessments of new and emerging risks, including risks involving multiple interdependencies. These risk assessments will:

- Identify specific examples of the nature, likelihood, and extent of the risk to BPS reliability and security (e.g., essential reliability services, loss of situational awareness, gas dependency, cyber and physical security, common mode failures larger than N-1, and loss of base-load units).
- Be objective, unbiased, focused, methodical, technically sound, and supported by rigorous analysis and quantification of risk.
- Present objective analysis of potential consequences.
- Provide actionable recommendations to mitigate significant risks and promote BPS resiliency.

The ERO Enterprise will conduct detailed special assessments that integrate:

- Interdependencies in addition to fuel-related, such as telecommunications and water supply.
- Analytic data trend insights regarding resiliency under severe weather conditions, identifying preventable aspects for BPS reliability.

The ERO Enterprise will also analyze data from geomagnetic disturbance events to further the understanding of their effects on the BPS to support enhancements to models and standards, and be prepared to address electromagnetic pulse events as necessary based on additional analyses.

These risk assessment efforts will require the ongoing cooperation, trust and support of industry, including (but not limited to) sharing of current and projected system data and support in technical and event analysis. Mechanisms must be put in place to track and assess the effectiveness of recommended mitigation measures.

The ERO Enterprise will collaborate with industry, industry forums, and other organizations to develop (1) a set of real-time indicators of interconnection health; (2) a list of key tasks and learning objectives for wide-area monitoring as well as assessing status following system events, including the expanded use of synchrophasor data; and (3) a supplement or companion to the *Interconnected Power System Dynamics Tutorial* that deals with wide-area monitoring under a changing resource mix. Additionally, the ERO Enterprise will work with industry and other stakeholders to expand the use of synchrophasor data, including the development of supplemental and back-up tools utilizing this data.

To achieve a leadership position in analyzing emerging complex risks, the ERO Enterprise will need to elevate its capabilities in advanced system and electronics engineering, larger scale data management, and advanced analysis methods and tools. Talent and tools are needed in power systems, system protection and control, renewable energy integration, power electronics, data analysis and cloud computing, telecommunications, information systems, probabilistic analysis and modeling, statistics, distribution systems, and cyber and physical security. Understanding of markets and policies affecting the generation mix, the location and growth of renewables, demand, fuel supply, and technology is also important.

While developing internal talent and resources will be an important area of focus, establishing, expanding, maintaining relationships with, and leveraging the expertise of industry and other organizations is also critical. Participation by stakeholders with the necessary expertise to understand the technical nature of the changes that are occurring, any associated risks, as well as the pros and cons of mitigation options, is critical. The ERO Enterprise will work with and leverage the resources and expertise of NERC's technical committees, industry, the Electric Power Research Institute (EPRI), the U.S. DOE, federal labs, universities, governmental institutions, technology and manufacturing companies, and other impacted and affected industries to advance reliability research and analytics to effectively and efficiently address these skill-based needs. The ERO Enterprise will work with standards drafting teams, industry, and other stakeholders to include the consideration of the impact of changing requirements in workforce skills and training in the standards development process.

Focus Area 4: Promote Leading Security Practices, Information Sharing and Analysis, and Resilience

The protection and resiliency of facilities and systems critical to maintaining BPS reliability is an important objective shared by both industry and the ERO Enterprise. NERC's physical security Reliability Standards require users, owners, and operators of the BPS to conduct risk assessments to identify critical facilities and develop and implement plans to protect those facilities from attacks. The electric sector remains the only critical infrastructure subject to mandatory, enforceable cyber

security standards. For example, the International Electrotechnical Commission's (IEC) 61850 Standard, titled "Communication Networks and Systems for Power Utility Automation," is being implemented throughout industry. As the use of more distributed controls systems become a more common practice, the IEC 61850 protocols will need to be deployed with an eye towards ensuring continued and enhanced cyber security. Best practices on these deployments need to be developed and shared broadly across the industry.

While standards and risk-based compliance and enforcement play an important role in addressing BPS physical and cyber security risks, there is widespread recognition that standards alone will not be adequate. Accurate and timely information sharing regarding current and emerging threats, prevention, response, and mitigation and recovery strategies is critical.

Over the past several years, the Electricity Information Sharing and Analysis Center (E-ISAC) has focused on improving its technical and analytical capabilities with a goal of becoming the electricity industry's leading and trusted source for analysis and sharing of security information[7]. At the request of the NERC Board and under the guidance of the ESCC and MEC, executive leadership of the E-ISAC developed a long-term strategic plan[8] to transform the E-ISAC into a world-class intelligence collecting and analytical organization for the electricity industry. This strategic plan was subsequently endorsed by both the MEC and NERC's Board. Consistent with this strategy, the E-ISAC will focus on the following objectives:

- Becoming an indispensable resource to electricity stakeholders in the United States, Canada, and Mexico for security information sharing and analysis;
- Building a highly engaged community of security professionals in the electric sector;
- Developing intelligence collecting and analytical capabilities that industry cannot do without;
- Achieving a maturity level where industry completely trusts the E-ISAC to gather, hold, analyze, and distribute highly sensitive security information; and
- Leveraging and working in partnership with industry, governmental agencies, and relevant and leading public and private organizations.

Resilience has become a critical element of BPS reliability. BPS resilience may be affected by not only emerging, cyber, and physical security risks, but also more traditional BPS risks. From 2012 to 2016, the ten most significant events each year (50 events total) were weather related. Although this indicates excellent performance by industry and the ERO Enterprise on reliability risk mitigation, it also points out a significant opportunity. The ERO Enterprise will expand its capability to use detailed information from events to be able to provide cause analysis and reliability assessment reports that can highlight priorities for improving grid resilience from catastrophic events. The ERO

[7] Significant support from the Electricity Subsector Coordinating Council (ESCC), the ESCC Members Executive Committee (MEC), the U.S. DOE, and other stakeholders have helped the E-ISAC be responsive to the industry's needs in order to provide unique insights, leadership, and coordination for security matters.

[8] E-ISAC Long-Term Strategic Plan (under Public Document Library)

Enterprise already supports resilience through GridEx, a grid security conference, and collaboration with other forums.

The ERO Enterprise will work closely with applicable governmental agencies, including (but not limited to) the Departments of Energy and Homeland Security, the ESCC, industry forums, and trade associations to support key physical and cyber security and resiliency information sharing and knowledge transfer initiatives, including the identification and promotion of best practices to improve resiliency when responding to extreme events.

To support the further mitigation of physical and cyber security vulnerabilities, the ERO Enterprise will:

- Conduct special regional assessments that address natural gas availability and pipeline impacts under physical attack scenarios.
- Better understand the interdependence of the telecommunication infrastructure and electric infrastructure during a natural disaster.
- Foster the development and communication of methods, models, and tools to simulate system reliability impacts for the planning and operational planning time horizons.
- Develop a feedback mechanism from the implementation of the critical infrastructure protection (CIP) standards to evaluate its effectiveness and lessons learned from technology deployment.
- Work with industry and other stakeholders to develop agreed-upon levels of cyber-resilience suitable for BPS planning and operations.
- Develop methods, models, and tools to simulate cyber impacts on system reliability, enabling BPS planning to withstand an agreed-upon level of cyber resiliency.
- Develop industry operating guidelines that incorporate an agreed-upon level of cyber resilience.

To facilitate preparedness, the ERO Enterprise will consider preparing sensitivity analyses to simulate the impacts from the most extreme natural events experienced to date.

Focus Area 5: Knowledge Transfer and Effective Communications

With all of the new players in a new reliability ecosystem, the scope of outreach and communications must be expanded to ensure that industry, policymakers, and other stakeholders benefit from the knowledge and information that the ERO Enterprise is capable of sharing to support our shared goal of understanding and ensuring BPS reliability. As the ERO Enterprise gains leadership in identifying new risks to reliability and security and develops new analytic approaches and results, it will be important to transfer that knowledge to key players and increase public understanding of the work the ERO Enterprise and industry does to maintain and enhance a highly reliable BPS, including addressing emerging risks. In addition to traditional reliability stakeholders, the ERO

Enterprise will engage with policymakers, governmental authorities, trade associations, equipment manufacturers and vendors, universities, laboratories and test facilities, and many others.

The role of sharing technical knowledge and results for the purpose of ensuring BPS reliability will also require a broader communication strategy, including communication with organizations that may have not traditionally been viewed as affecting or having knowledge and information that is important to reliability.

Strengthen Engagement across North America (Focus Area 6)

Focus Area 6: Strengthening Engagement across North America

NERC and the Regional Entities with cross-border footprints will maintain robust engagement with their members and pursue a strategy with goals and activities in support of the overall strategic initiatives of the North American-wide ERO Enterprise in order to maintain and enhance the value of the international ERO model. In recognition of the increased reliability and security interdependencies among the United States, Canada, and Mexico, the ERO Enterprise will focus on the following:

- **Consistency**: Ensure a comparable level of reliability and security exists for the BPS in North America in a way that recognizes the uniqueness of jurisdictional regulatory environments in all applicable program areas, including adoption of standards; risk-based compliance monitoring and enforcement; and reliability assessments.
- **Transparency**: With due consideration of appropriate mechanisms to protect confidentiality where necessary, ensure transparency in both directions for information about reliability risks, including compliance violations and mitigation, events, and data needed to assess reliability.
- **MOUs**: Working with Canadian authorities, where necessary update existing MOUs to verify references to current applicable provincial laws, established practices, and agreed upon priorities of the ERO Enterprise and provincial regulators.
- **Expertise:** Ensure relevant expertise from the United States, Canada, and Mexico is fully integrated in ERO Enterprise technical and standards development activities.

For Mexico, the ERO will complete a full integration of Mexico into the ERO and ensure that Mexico is engaged with NERC and relevant Regional Entity technical committees and initiatives, including:

- Analysis of reliability standards and process development;
- Assessment of reliability performance and risks;
- Identification and assessment of risks related to critical infrastructure protection, cyber, and physical security; and
- Sharing of relevant reliability information associated with Mexico's accelerated development of renewable energy resources and transmission infrastructure.