NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Board of Trustees

December 12, 2019 | 2:00-3:00 p.m. Eastern
Conference Call

Participant Dial-in: 1-800-458-4148 | Conference ID: 9230281

Webex: www.readytalk.com | Code: 4469686 | Click Join

Call to Order

NERC Antitrust Compliance Guidelines

Introductions and Chair's Remarks

1. **2019 Long-Term Reliability Assessment* – Accept**
2. **ERO Enterprise Long-Term Strategy* – Approve**
3. **Supply Chain Standards Effectiveness Review* – Information**
4. **Other Matters and Adjournment**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

2019 Long-Term Reliability Assessment

Action

Accept the report, endorse the recommendations contained therein, and authorize its publication.

Background

The Long-Term Reliability Assessment (LTRA) is developed annually by NERC and Regional Entity Staff in accordance with the Electric Reliability Organization's (ERO) Rules of Procedure and Section 215 of the Federal Power Act, which instructs the ERO to conduct periodic assessments of the North American bulk power system (BPS). The 2019 LTRA provides a platform for the ERO to discuss emerging reliability issues and for industry to document its plans to maintain reliability during the next 10 years. The ERO's primary objective in this effort is to independently identify and assess issues that may impact the reliability of the BPS. The scope of the assessment includes the following:

- Review, assess, and report on the overall electric generation and transmission reliability (adequacy and operating reliability) of the interconnected BPS, both existing and as planned.
- Assess and report on the key issues, risks, and uncertainties that affect or have the potential to affect the reliability of existing and future electric supply and transmission.
- Review, analyze, and report on self-assessments of electric supply and bulk power transmission reliability, including reliability issues of specific Regional concern.
- Identify, analyze, and project trends in electric customer demand, supply, and transmission and their impacts on BPS reliability.
- Investigate, assess, and report on the potential impacts of new and evolving electricity market practices, new or proposed regulatory procedures, and new or proposed legislation (e.g. environmental requirements) on the adequacy and operating reliability of the BPS.

Summary

The electricity industry provided the ERO with resource adequacy projections for the 2020–2029 assessment period. The ERO independently assessed these projections and has identified key findings and recommendations. In summary, the ERO found that the BPS is undergoing a rapid and significant transformation with ongoing retirements of fossil-fired and nuclear generation, as well as growth in new natural gas, wind, and solar resources. This shift is caused by several drivers, such as federal, state, and provincial policies, low natural gas prices, electricity market forces, and integration of both distributed and utility-scale renewable resources. The changing resource mix alters the operating characteristics and constraints of the BPS and these changing characteristics must be well understood and incorporated into planning to assure continued reliability.

ERO Enterprise Long-Term Strategy

Action
Approve

Background
As discussed during the August 14, 2019, MRC meeting, the *ERO Enterprise Long-Term Strategy*, which was last approved by the Board of Trustees (Board) on November 9, 2017, was recently reviewed and revised by ERO Enterprise leadership as part of an effort to streamline its strategic and operational documents and ensure alignment with the Reliability Issues Steering Committee's (RISC's) currently identified bulk power system (BPS) risks. A draft was posted for stakeholder comment from September 10–October 1, 2019. The draft included the following ERO Enterprise value drivers and long-term focus areas:

Value Drivers

- Organizing and deploying top talent
- Developing and delivering innovative and risk-based programs and tools
- Collaborating effectively with industry and other stakeholders
- Maintaining independence and objectivity

Long-Term Focus Areas

1. Expand risk-based focus in all standards, compliance monitoring, and enforcement programs
2. Assess and catalyze steps to mitigate known and emerging risks to reliability and security, leveraging the RISC's biennial *ERO Reliability Risk Priorities Report* (RISC report)
3. Build a strong, Electricity Information Sharing and Analysis Center (E-ISAC)-based security capability
4. Strengthen engagement across the reliability and security ecosystem in North America
5. Capture effectiveness, efficiency, and continuous improvement opportunities

Summary
Based on comments received and additional input from the NERC and Regional Entity boards, the long-term strategy was further revised from the version posted for comment to (1) add desired outcomes for each ERO Enterprise value driver; (2) distinguish between near-term and longer-term tasks; (3) increase references to the ERO Enterprise's role with respect to BPS resilience; (4) more closely align discussion of BPS risks with those identified in the RISC report (accepted on November 5, 2019); and (5) enhance discussion related to the importance of the ERO Enterprise's engagement and communications with the key players of the reliability and security ecosystem.

The revised *ERO Enterprise Long-Term Strategy* has been socialized with each Regional Entity board and is enclosed for Board approval at its December 12, 2019, meeting.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Long-Term Strategy

Approved by the NERC Board of Trustees on [Date]

Introduction and Background

Electricity is a vital component of the fabric of modern society. The Electric Reliability Organization (ERO) Enterprise, which consists of the North American Electric Reliability Corporation (NERC) and the six Regional Entities,[1] serves to strengthen that fabric for the benefit of nearly 400 million North American citizens. Working with users, owners, and operators of bulk power system (BPS) assets, government partners, and other stakeholders and industry participants, the ERO Enterprise pursues its **mission of assuring the effective and efficient reduction of risks to the reliability and security of the BPS**.

NERC and the Regional Entities play different, but important and complementary roles in delivering ERO Enterprise programs. NERC provides industry-wide perspective and oversight, and the Regional Entities have unique features and activities that serve the needs of their regional constituents, while ensuring that industry follows NERC and Regional Reliability Standards. The ERO Enterprise is explicitly committed to its collective success in achieving its **vision of a highly reliable and secure North American BPS**.

The ERO Enterprise has matured significantly since its inception. In addition, since the *ERO Enterprise Long-Term Strategy* was last approved by the NERC Board of Trustees in 2017, the ERO Enterprise has undergone significant social and structural change. With the dissolution of the Southwest Power Pool Regional Entity and Florida Reliability Coordinating Council Regional Entity, their registered entity footprints have been consolidated with MRO and SERC, and the ERO Enterprise now encompasses six organizations of more similar size and complexity. These and other changes have also created the opportunity to refresh and improve the interactions between and among the ERO Enterprise entities.

With the collective mission and vision, the regional model is critical to the ERO Enterprise's success. NERC and the Regional Entities are partners through which the Enterprise will succeed, and are committed to:

- Working together as one team and honoring each of its roles;
- Actively supporting ERO Enterprise activities while eliminating unnecessary duplication of work;
- Collaborating in developing clear and consistent guidance across the ERO Enterprise;
- Sharing information, knowledge, and resources across the ERO Enterprise;
- Developing and sharing harmonized messages across ERO Enterprise communications; and
- Supporting innovation, initiatives, and the sharing of best-practices across the ERO Enterprise.

[1] The Regional Entities include the Midwest Reliability Organization (MRO), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity (Texas RE), and Western Electricity Coordinating Council (WECC).

ERO Enterprise Value Drivers

The electricity industry is experiencing significant policy and technical forces that are driving rapid change in how electricity systems are designed, planned, operated, and secured. The transformed reliability and security ecosystem will include new risks, new complexities, new terminology, new requirements, new players, and jurisdictional challenges. The ERO Enterprise will anticipate and respond to these changes, identify risks and their mitigation, and, using the unique nature of the North American footprint, adapt during the five-to-seven-year horizon.

In light of this changing industry landscape and, leveraging the strengths of the regional model that allow for alignment with respect to each entity's individualities, the ERO Enterprise will focus on four key value drivers to achieve its vision and effectively pursue its mission with desired outcomes:

Value Driver	Outcome
• Organizing and deploying top talent	Recognized as the center of independent reliability and security knowledge and excellence with extensive engineering and analytical expertise
• Developing and delivering innovative and risk-based programs and tools	As reliability and security risks emerge quickly, coordinated and swift development of improved processes, tools, and simulation models provide a strong foundation and catalyst to mitigate these risks
• Collaborating effectively with industry and other stakeholders	New and effective ways to engage key subject matter experts among its stakeholder community and partnerships with other organizations enable access to the expertise needed to address reliability and security risks
• Maintaining independence and objectivity	A trusted resource by its government partners, as well as industry, and all participants are treated fairly and equitably

More detail on each of these key value drivers is provided below.

- **Organizing and deploying top talent** to address increasingly complex issues and skillfully execute the ERO Enterprise programs in a rapidly changing industry environment. The ERO Enterprise will be recognized as the center of independent reliability and security knowledge and excellence by providing extensive engineering and analytical expertise. To this end, the ERO Enterprise will attract, retain, and develop top talent to perform its mission-critical roles. As important as its staff and capabilities are, the ERO Enterprise recognizes that its work is more valuable when it is done with the appropriate industry context. Further, the expertise that stakeholders bring is central to the ERO Enterprise's work; therefore, the ERO Enterprise will also focus on enhancing engagement with key subject matter experts, representing multiple areas, such as power systems planning, operations, security, resilience, and economics. Talent management is essential, and the ERO Enterprise is committed to using increasingly specialized resources effectively and efficiently and leveraging the capabilities it stewards.

- **Developing and delivering innovative and risk-based programs and tools** to effectively address the highest risks to BPS reliability, resilience, and security. The electricity industry is evolving rapidly as the resource mix shifts away from traditional baseload, mid-merit, and peaking assets with assured fuel supplies. The system is much more dependent on variable energy resources (e.g., wind and solar), balanced by natural gas, hydro, and oil, with a significantly diminished role for traditional solid fuel generation (e.g., coal and nuclear). Significant resource development is also occurring within the distribution system, where customer participation in load management and resource addition programs add significant planning and operating complexity to the grid. And while the increasing use of digital control technologies brings new efficiencies to the electricity sector, it can also increase the security risk and cyber and physical attack surface. Further, as the system transforms, ensuring the desired level of resilience is an important part of the continued reliable operation of the BPS.

  The ERO Enterprise and industry subject matter experts continuously collaborate to identify BPS risks, recommend and deploy mitigations, and monitor results toward assuring that the risks to reliability are mitigated to desired levels. However, as technology integration accelerates, reliability and security risks emerge quickly, requiring a similar response speed for their mitigation. Coordinated and swift development of improved processes, tools, and simulation models must be part of industry's response, and the ERO Enterprise will provide a strong foundation and catalyst to support this response.

- **Collaborating effectively with industry and other stakeholders** to ensure the work of the ERO Enterprise is relevant, addresses the key issues of the reliability, resilience, and security ecosystem, and is conducted in the appropriate context and with the required subject matter expertise. Stakeholder engagement is critical to the success of the ERO Enterprise's mission. The ERO Enterprise will continue to find new and effective ways to engage key subject matter experts among its stakeholder community, and will increase the effectiveness of its partnerships with other organizations that share in its reliability and security mission.

- **Maintaining independence and objectivity** to enable the ERO Enterprise to be the voice of reliability and security. The ERO Enterprise preserves its objectivity and independence to call "balls and strikes" as it sees them and be a trusted resource by its government partners. In addition, the ERO Enterprise's independence serves to assure industry that all participants are treated fairly and equitably, and in a manner that is not biased toward any specific technology, sector, or entity.

The leadership of the ERO Enterprise has embraced these four value drivers as being foundational to how it will achieve collective success in meeting its mission of reducing risks to BPS reliability and security, in concert with the long-term focus areas described below.

Long-Term Focus Areas

The ERO Enterprise has identified five key strategic focus areas and desired outcomes for the coming years:

Focus Area	Outcome
1. Expand risk-based focus in all standards, compliance monitoring, and enforcement programs	Continued high BPS reliability and security with no identified gaps in Reliability Standards
2. Assess and catalyze steps to mitigate known and emerging risks to reliability and security, leveraging the NERC Reliability Issues Steering Committee's (RISC's) biennial *ERO Reliablity Risk Priorities Report* (RISC report)	Clearer understanding of emerging risks to the BPS and associated mitigation strategies, particularly for BPS risks originating from events on the distribution system and cyber attacks
3. Build a strong, Electricity Information Sharing and Analysis Center (E-ISAC)-based security capability	Full implementation of the *E-ISAC Long-Term Strategic Plan* and industry-wide recognition of the E-ISAC value proposition
4. Strengthen engagement across the reliability and security ecosystem in North America	Effective relationships with industry trade groups and forums, federal, state, and provincial regulators, and the broader reliability and security ecosystem
5. Capture effectiveness, efficiency, and continuous improvement opportunities	Quantitative and qualitative results from current ERO Enterprise effectiveness and efficiency initiatives and distinct methods for ongoing effectiveness and efficiency evaluation

More detail on each of these focus areas is provided below.

Focus Area 1: Expand Risk-Based Focus in Standards, Compliance Monitoring, and Enforcement

NERC facilitates development of Reliability Standards that establish threshold reliability, resilience, and security requirements to assure the Bulk Electric System (BES) is planned, operated, maintained, and secured to minimize risks of cascading failures, avoid damage to major equipment, or limit interruptions of the BPS. The ERO Enterprise ensures that owners and operators of the BES comply with the Reliability Standards through registration, certification, compliance monitoring, mitigation, and enforcement activities that are part of the Compliance Monitoring and Enforcement Program (CMEP). Over the past several years, the ERO Enterprise has transitioned to a risk-based approach for standards and CMEP activities, prioritizing and focusing resources on significant BPS reliability risks. The ERO Enterprise will continue to uphold and expand this risk-based focus through the following:

- Through ongoing standards development and review processes (such as the Standards Efficiency Review), ensure Reliability Standards are clear, timely, considerate of costs, effective in mitigating material risks, and do not unnecessarily burden industry with administrative requirements and/or detract from reliability or security;
- Use the full suite of tools (e.g., NERC alerts, assist visits, best practice webinars, white papers, lessons-learned guidelines) to provide guidance to industry as to how to mitigate emerging risks,

evaluating the effectiveness of such approaches and if new or modifications to Reliability Standards are necessary;

- Continue to improve quality and consistency of risk assessments and internal controls reviews, and ensure Compliance Oversight Plans for registered entities use the appropriate set of tools (audits, certifications, spot checks, etc.) at the appropriate frequency to (1) support a culture of reliability and security and (2) provide reasonable assurance that entities are in compliance with applicable Reliability Standards;
- Focus enforcement efforts on highest risk violations and continue to find ways to efficiently process and close out lower risk violations; and
- Along with delivery of the CMEP tool, Align, enhance security and alignment in practices and outcomes across all Regional Entity CMEP efforts.

Focus Area 2: Assess and Catalyze Steps to Mitigate Known and Emerging Risks to Reliability and Security

The ERO Enterprise works closely with industry, industry forums, government, and other organizations that focus on BPS reliability, and is part of the reliability and security ecosystem to perform ongoing analysis of significant known reliability risks, such as vegetation management, protection system misoperations, cybersecurity, human error, and system stability. The ERO Enterprise also collaborates with these subject matter experts and other ecosystem participants as appropriate to assess emerging risks that result from (1) grid transformation (e.g., expansion of variable and distributed energy resources and integration of digital controls and new technologies, such as energy storage and inverter-based resources); (2) extreme natural events; (3) security vulnerabilities (both cyber and physical); and (4) critical infrastructure interdependencies (e.g., fuel sufficiency). Lastly, to support its advanced analytics, the ERO Enterprise collects substantial amounts of data and information on the ongoing performance of the BPS, along with projected system conditions.

A key driver to these analyses and assessments is the biennial RISC report, which includes risk prioritization and mitigation recommendations. Leveraging the RISC report and the ERO Enterprise's ongoing data collection, the ERO Enterprise will continue to identify and address these risks through its analysis, assessment, and situation awareness activities. The ERO Enterprise will also continue its increased focus on enhancing BPS resilience, including the industry's ability to prepare for, withstand, and recover from extreme contingency events.

Risk mitigation recommendations identified by the ERO Enterprise often require improved processes, tools, and simulation model development that are delivered in a timely, actionable, and forward-looking manner. A robust feedback loop from recommendation to action is critical to the ERO Enterprise's mission of assuring reliability and security. To address this, the ERO Enterprise will partner with industry stakeholders to strengthen the feedback loop toward ensuring that recommended processes, tools, and simulation models are systematically developed and delivered.

In support of these risk identification, analysis, and mitigation activities, the ERO Enterprise will focus on the following:

- Build appropriate outreach, training, and education to registered entities through NERC and the Regional Entities to reduce the incidence of known risks to reliability;
- Convene, fund as necessary, and influence the technical reliability and security ecosystem to develop and deliver the necessary tools and programs for data collection, modeling, analytics, and risk-based programs that address existing and emerging risks;
- Undertake special assessments and studies, including case-specific examples of real and potential impacts, to understand emerging risks from new technologies, and launch appropriate task forces to develop mitigation options. Some of these efforts may be in collaboration with state regulators, policymakers, and stakeholders, such as the National Association of Regulatory Utility Commissioners (NARUC), focusing on distributed energy resources and other risks emanating from events or conditions on the increasingly integrated distribution system that may cause cascading of the BPS;
- Integrate NERC and Regional Entity assessments to ensure that identified risks are being properly addressed, and continue to monitor those risks to understand region-specific expressions of industry-wide issues and impacts;
- Develop measures of BPS and cyber resilience, including the ability to prepare for, withstand, and recover from extreme contingencies, such as high-impact, low frequency events, and identify processes and approaches to enhance resilience through NERC's reliability and security toolkit as well as industry action. Work in collaboration with the forums and Department of Energy (DOE);
- Strengthen the analysis of cyber impacts on the BPS by enhancing industry's planning capabilities to reduce cyber vulnerabilities and mitigate impacts of cyberattacks on future systems, including improvements made from supply chain enhancements and corrective actions in system design. Enhance industry's ability to develop approaches to pre-position the system when under attack and explore recovery strategies; and
- Use data analytics, research, and relationships with other critical infrastructures to identify leading indicators of emerging risks and the potential harm of currently unknown risks, and prioritize and communicate these to industry for awareness and mitigation.

Focus Area 3: Build a Strong, E-ISAC-Based Security Capability

In addition to standards and CMEP activities associated with cyber and physical security, the ERO Enterprise supports the E-ISAC and its programs. While the E-ISAC is operated by NERC under a strict Code of Conduct, the Regional Entities benefit from the E-ISAC programs through their participation in the Cybersecurity Risk Information Sharing Program (CRISP) and contribute to the ERO Enterprise's security mission through education and outreach.

The E-ISAC works with North American electricity asset owners and operators, government partners, cross-sector and international entities, and the supply chain community to develop and share information to foster BPS resiliency through security. It engages with government partners to help de-classify sensitive security information and add the context needed to protect electricity sector devices and assets. Through its own long-term strategy, the E-ISAC has focused on improving its technical and analytical capabilities

with the goal of becoming the electricity industry's leading and trusted source for analysis and sharing of security information. The E-ISAC will continue its growth as follows:

- Ensure the *E-ISAC Long-Term Strategic Plan* is executed such that the E-ISAC is viewed by industry as meeting its needs as one of its key trusted sources of security information:
  - Encourage electricity asset owners and operators and government partners to share relevant security information for deeper analysis and mitigation development for a robust common defense of the grid;
  - Expand the E-ISAC's reach (membership) through member engagement and outreach; and
  - Continue to innovate outbound communication vehicles to get important and actionable insights into the hands of chief executive, operating, information, and security officers and their staffs in a timely manner;
- Build strong connectivity and engagement with the Electricity Subsector Coordinating Council and, in concert with the Members Executive Committee, evolve the E-ISAC long-term strategy as appropriate to stay relevant to industry's needs;
- Continue to mature the E-ISAC business processes and controls and develop performance metrics to evaluate the performance of the E-ISAC and its impact on industry's security risk profile;
- Collaborate with other sectors' security infrastructure where appropriate (e.g., the Financial Systemic Analysis and Resilience Center and the Downstream Natural Gas Information Sharing and Analysis Center) to facilitate cross-sector information sharing and threat analysis; and
- Strengthen relationships and intelligence sharing with key government agencies, such as the DOE as the U.S. electricity sector-specific agency, the Department of Homeland Security (DHS), as well as Natural Resources Canada (NRCan), Canada's Communications Security Establishment, and Mexico's Secretaría de Energía (SENER).

Focus Area 4: Strengthen Engagement across the Reliability and Security Ecosystem in North America

The ERO Enterprise engages with key players in the reliability and security ecosystem, including industry subject matter experts, trade associations and forums, policymakers and government partners, equipment manufacturers and vendors, and universities and laboratories to ensure (1) the work of the ERO Enterprise is collaborative, informed, relevant, and performed in the appropriate context and (2) these players benefit from the knowledge and information the ERO Enterprise is capable of sharing to support the goal of understanding and assuring BPS reliability and security. NERC and the Regional Entities with cross-border footprints maintain robust engagement with their Canadian and Mexican members and pursue goals and activities in support of the overall strategic initiatives of the North American-wide ERO Enterprise.

As new players become part of the changing reliability and security ecosystem, the scope of outreach will be expanded to include collaboration and communication with organizations important to North American BPS reliability and security. In recognition of the increased reliability and security

interdependencies among these key players, and to continue the engagement critical to ERO Enterprise success, the ERO Enterprise will:

- Nurture relationships with key industry trade associations, as well as those associations representing technology, affiliated sectors, and end users to understand context and leverage their experience and reach;
- Collaborate effectively with other non-profit organizations that share elements of the ERO Enterprise's reliability and security mission, and seek out and work with representatives of academia, other critical infrastructures, and international experts to broaden the ERO Enterprise's collective knowledge and awareness of current and unknown risks and strategies to address them;
- Leveraging the Regional Entities' specialized and localized point of view, strengthen and expand outreach, coordination, and collaboration with state energy regulators and related offices to address risks to reliability stemming from the relocation of resources and interdependency between the operations of distribution and the BPS; and
- Strengthen proactive outreach and communications with key provincial, federal, and state regulatory, legislative, and policy bodies and associations across North America:
  - In the United States:
    - In executive and legislative roles, the DOE, the DHS, the Department of State and related agencies, as well as congressional committees with jurisdiction responsible for reliability and security matters related to the BPS and the E-ISAC;
    - In regulatory roles, the Federal Energy Regulatory Commission offices, including the Office of the Chairman and Commissioners, Office of Electric Reliability, and related offices; and
    - For states, NARUC to include coverage at regional meetings, as well as state energy regulators and state associations (e.g., the National Governors Association, Western Governors Association, Council of State Governments, and National Conference of State Legislatures);
  - In Canada, leveraging the relationships built through the cross-border Regional Entities, improve consistency and visibility and assure high reliability and security performance of Canadian entities through relationships and connectivity with:
    - Canada's Energy and Utility Regulators (CAMPUT) and individual provincial regulators and government partners, recognizing the strong independence of provincial energy policy and regulation among Canadian provinces; and
    - Canadian federal institutions, such as NRCan, the National Energy Board, the Canadian Security Intelligence Service, Public Safety Canada, and the Department of National Defence;
  - In Mexico, continue to work toward integration as interconnections with the North American grid occur by monitoring and staying engaged with:
    - The Mexican industry evolution; and

- Mexican industry partners, including the Comisión Reguladora de Energia, Centro Nacional de Control de Energía, and SENER.

Focus Area 5: Capture Effectiveness, Efficiency, and Continuous Improvement Opportunities

The ERO Enterprise embraces consistency, quality, efficiency, and timeliness of results, and recognizes that improvements in efficiency are essential to mitigating the ongoing cost of maintaining and improving the quality and effectiveness of ERO Enterprise operations. To that end, the ERO Enterprise understands it must routinely and systematically review major processes to promote operational excellence and identify and implement efficiency improvements. The ERO Enterprise will support this objective as follows:

- With the oversight of each of its boards, continue to identify internal effectiveness, efficiency, and program maturity improvements in each of the ERO Enterprise corporations and reflect these in the annual business plan and budget process, share lessons learned and best practices, and collaborate on Enterprise-wide efficiencies;
- In the near term, focus on the "big three" effectiveness and efficiency opportunities:
  - Execute the Standards Efficiency Review initiative and ongoing review of Reliability Standards for effectiveness and compliance efficiency;
  - Successfully deploy the CMEP Align tool to capture the identified effectiveness, security, consistency, and efficiency benefits built into its business case; and
  - Evolve ERO Enterprise stakeholder engagement to ensure the best expertise works on the right set of issues in the most time-efficient and cost-effective manner while ensuring meaningful opportunities for stakeholder engagement;
- In the long term:
  - Evaluate current processes and practices to ensure they add value and contribute to the mission, and identify, prioritize, and deploy all tools available to the ERO Enterprise to achieve the mission;
  - Catalyze development of proactive solutions to emerging risks to the greatest extent possible; and
  - Continue to look for "the next wave" of strategic effectiveness and efficiency opportunities while ensuring resources are focused on key reliability and security challenges.

Conclusion

As the reliability and security ecosystem changes, the ERO Enterprise is in a unique position to support industry in ensuring North American BPS reliability, resilience, and security. The key value drivers and focus areas outlined above are intended to guide the ERO Enterprise over multiple business planning and budgeting cycles. ERO Enterprise leadership will revisit these areas periodically to ensure the long-term strategy's relevancy and efficacy, particularly in response to any changes to the ERO Enterprise landscape, as well as emerging reliability and security risks captured through the ERO Enterprise's ongoing monitoring of reliability and the RISC's processes and biennial report.

Supply Chain Standards Effectiveness Review

Action

Information

Plan for Effectiveness Review

NERC plans to measure the effectiveness of the Supply Chain Standards by performing the following actions during the first two years of implementation:

ERO staff will conduct surveys on supply chain awareness, compiling statistics on identified key risk indicators. These indicators include 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. Information compiled will be examined for trends and reported periodically to the Reliability and Security Technical Committee and posted on the website.

ERO staff will solicit comparative contractual language (pre and post Supply Chain Standards implementation) voluntarily from entities 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. This will include entities not subject to the Supply Chain Standards to determine whether there has been any incidental benefits derived from the implementation of the Supply Chain Standards.

Finally, ERO staff will analyze supply chain communications, education, outreach, and training to determine whether vulnerabilities have been identified and successfully communicated. This will include inquires to the E-ISAC on supply chain issues and requests for training and outreach.

At the conclusion of the two years, NERC staff will report to the Board on its analysis of the effectiveness and provide any recommended actions that may be determined to be necessary.

Background

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829, directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations, as follows:

> *[The Commission directs] NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. (P. 45)*

Following the issuance of Order No. 829, NERC staff initiated Reliability Standards Project 2016-03 to address supply chain risk management in the Critical Infrastructure Protection (CIP) standards. The project resulted in the development of new standard CIP-013-1, and modifications in CIP-005-6 and CIP-010-3 (collectively, the Supply Chain Standards). The Supply Chain Standards support reliability by requiring entities to implement plans and processes to mitigate supply chain cyber security risks to high and medium impact assets. Following industry approval of the Supply Chain Standards on July 20, 2017, the Board of Trustees (Board) adopted the Supply Chain Standards at its August 10, 2017 meeting. FERC approved the Supply Chain Standards with directives for additional modifications in Order No. 850, issued October 18, 2018.[1]

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to implementation and risk evaluation.[2] The resolutions outlined in detail six actions by NERC management and stakeholders to assist in the implementation and evaluation of the Supply Chain Standards, as well as other actions to address potential supply chain risks for assets not currently subject to the standards. One of those resolutions directed NERC management, collaborating with NERC technical committees and other experts, to develop a plan to evaluate the effectiveness of the Supply Chain Standards, as described in the resolution, and report to the Board.

In 2019 ERO staff conducted a series of small group advisory sessions on supply chain, including the Supply Chain Standards, and solicited feedback on the subject. This feedback was used to assist in developing the plan.

[1] Order No. 850, *Supply Chain Risk Management Reliability Standards*, 165 FERC ¶ 61,020 (2018).

[2] The Proposed Additional Resolutions for Agenda Item 9.a: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1, NERC Board of Trustees Meeting, August 10, 2017, is available at: http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.