NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 15, 2020

Ms. Jennifer Sterling, Chair
NERC Member Representatives Committee

Dear Jennifer:

I invite the Member Representatives Committee (MRC) to provide policy input on a matter of particular interest to the NERC Board of Trustees (Board) as it prepares for its August 19-20, 2020, meetings, which will occur via teleconference due to the coronavirus (COVID-19) outbreak. In addition, policy input is requested on any items on the preliminary agendas for the quarterly Board, Board Committees, and MRC meetings. The preliminary agendas are included in the MRC Informational Session agenda package (see Item 2) and are attached hereto (**Attachment A**). The MRC's August agenda includes an opportunity for MRC members to provide additional input to the Board on the final agenda and materials. **As a reminder, please include a summary of your comments in your response (i.e., a bulleted list of key points) for NERC to compile into a single summary document to be provided to the Board for reference, together with the full set of comments.**

Electricity Information Sharing and Analysis Center (E-ISAC) Long-Term Strategic Plan
In 2017, the E-ISAC developed the E-ISAC's Long-Term Strategic Plan, with guidance from the ESCC Member Executive Committee (MEC) and other stakeholder groups. The purpose of the Strategic Plan was to better define the E-ISAC's mission and priorities, and focus its resources to help the electric sector protect against and mitigate the risks of escalating cyber and physical security threats. In April and May 2017, respectively, the MEC endorsed and the Board accepted the Strategic Plan.

As part of management's planning efforts for 2020 and 2021, the E-ISAC assessed the Strategic Plan to: (1) measure the E-ISAC's progress to date; (2) confirm the E-ISAC's strategic and operational focus; (3) evaluate and refine its products and services; (4) optimize resource planning and allocation; and (5) identify additional areas to provide value to members. Working with the MEC, the E-ISAC updated the Strategic Plan based on this assessment (**Attachment B**). In updating the Strategic Plan, the E-ISAC conducted quantitative assessments of critical infrastructure ISACs to measure itself against those ISACs. A key finding of the assessment was that the E-ISAC is a well-established organization, with comparable resources and offerings to the top tier of the assessment group.

The updated Strategic Plan describes the E-ISAC's near-term and long-term strategic and operational focus. In the near-term (1-2 years), the E-ISAC's primary focus will be improving the effectiveness and efficiency of current products, platforms, and services. The E-ISAC will also sharpen its focus and execution in building and maintaining membership by demonstrating value through improved analysis,

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

timely sharing of actionable information, and collaboration with key government and strategic partners, while also ensuring that E-ISAC operations are both effective and efficient.

For the long-term horizon (3-5 years), the E-ISAC will focus on providing additional value to members and other stakeholders in four key areas: (1) enhancing its analytical capabilities (both internal and in partnership with third parties); (2) identifying, analyzing, and sharing operational technology risks and risk mitigation strategies; (3) developing enhanced capabilities to share critical threat and intelligence information to provide timely and actionable information to the sector; and (4) extending E-ISAC services and capabilities to support the downstream natural gas sector, given cross-sector interdependencies.

The E-ISAC will request MEC endorsement of the updated draft of the Strategic Plan during the MEC's meeting in July 2020 and Board acceptance of the Strategic Plan at the Board's August 2020 meeting.

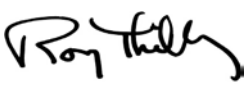
The Board requests MRC policy input on the following:

1. **Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?**
2. **Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members?**

At their August meetings, the MRC and Board will discuss and may take action to approve amendments to the NERC Bylaws. The proposed amendments will also be discussed at the MRC Informational Session on July 22, 2020. NERC management comprehensively reviewed the NERC Bylaws at the Board's request and identified the proposed revisions to clarify certain requirements, incorporate the Board's feedback on certain governance matters, improve internal document consistency, and align certain provisions with applicable law. An explanatory memo with a redline of the NERC Bylaws was distributed to MRC members on July 1, 2020 for review and comment. Any final clarifications will be identified at the MRC Informational Session. Following MRC and Board approval, NERC will file the proposed amendments with the Federal Energy Regulatory Commission for approval.

Written comments in response to the input requested above, the preliminary agenda topics, and on other matters that you wish to bring to the Board's attention are due by **August 5, 2020,** to Kristin Iwanechko, MRC Secretary (Kristin.Iwanechko@nerc.net). The formal agenda packages for the Board, Board Committees, and MRC meetings will be available on August 6, 2020, and the presentations will be available on August 13, 2020. The Board looks forward to your input and discussion of these matters during the August 2020 meetings.

Thank You,



Roy Thilly, Chair
NERC Board of Trustees

cc: NERC Board of Trustees
Member Representatives Committee

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Member Representatives Committee (MRC)

Pre-Meeting and Informational Webinar

July 22, 2020

RELIABILITY | RESILIENCE | SECURITY




Objectives – Pre-Meeting and Informational Session

- Review schedule and preliminary agenda topics for:
  - August 19 Board Committee (open) meetings
  - August 20 MRC meeting
  - August 20 Board of Trustees meeting
- Review policy input letter topic
- Receive updates on emerging and informational issues

Schedule of Quarterly NERC Conference Calls

Wednesday, August 19, 2020	
11:00 a.m.-12:00 p.m.	Corporate Governance and Human Resources Committee Meeting —**Open**
12:45-1:45 p.m.	Technology and Security Committee Meeting—**Open**
2:30-3:30 p.m.	Finance and Audit Committee Meeting—**Open**
Thursday, August 20, 2020	
11:00 a.m.-1:00 p.m.	Member Representatives Committee Meeting—**Open**
2:00 p.m.-4:00 p.m.	Board of Trustees Meeting—**Open**

Corporate Governance and Human Resources Committee
11:00 a.m. – 12:00 p.m., August 19

- COVID-19 Re-Entry Strategy
- 2020 ERO Work Plan Priorities Update
- Review Self-Assessment and MRC Assessment of Board of Trustees Effectiveness Survey
- Review Employee Reporting and Document Retention Policies and Procedures
- Human Resources and Staffing Update

Technology and Security Committee
12:45 p.m. – 1:45 p.m., August 19

- Review and Recommend Acceptance of E-ISAC Long-Term Strategic Plan
- ERO Enterprise Business Technology Projects Update
- ERO Enterprise Align Project Update
- ERO Enterprise Secure Evidence Locker Update

Finance and Audit Committee
2:30 p.m. – 3:30 p.m., August 19

- Second Quarter Unaudited Financial Statements
- Review and Recommend Approval of NERC and Regional Entity Proposed 2021 Business Plans and Budgets and Associated Assessments

Member Representatives Committee
11:00 a.m. - 1:00 p.m., August 20

- Schedule for MRC Officer and Sector Elections
- Election of NERC Trustee
- General Updates and Reports
  - Board of Trustees Nominating Committee Update
  - Business Plan and Budget Input Group Update
  - Regulatory Update
- Policy and Discussion Items
  - Responses to the Board's Request for Policy Input
    - E-ISAC Long-Term Strategic Plan
  - Approve NERC Bylaws Amendments
  - Additional Policy Discussion of Key Items from Board Committee Meetings
  - MRC Input and Advice on Board Agenda Items and Accompanying Materials

Member Representatives Committee
11:00 a.m. - 1:00 p.m., August 20

- Technical Updates
  - Update on FERC Reliability Matters
  - Update on Cloud Computing

Board of Trustees
2:00 p.m. - 4:00 p.m., August 20

- Report on August 18, 2020 Annual Meeting of the NERC Board of Trustees and Canadian Regulators
- Board Committee Reports
  - Accept Second Quarter Unaudited Financial Statements
  - Approve NERC and Regional Entity Proposed 2021 Business Plans and Budgets and Associated Assessments
  - Accept E-ISAC Long-Term Strategic Plan
- Standards Quarterly Report and Actions
  - Adopt WECC Variance to PRC-006-5
  - Adopt Project 2019-03 Cyber Security Supply Chain Risks
  - Approve NPCC Regional Standard Processes Manual Modifications
  - Supply Chain Activities Update
  - 2020 ERO Enterprise Dashboard Update

Board of Trustees
2:00 p.m. - 4:00 p.m., August 20

- Other Matters and Reports
  - Discuss Policy Input and Member Representatives Committee Meeting
  - Approve Rules of Procedure Amendments for Second Five-Year Performance Assessment Compliance Filing
    - Registration and Certification: Section 500 and Appendices 2, 5A, 5B, & 5C
    - E-ISAC: Section 1003
    - Sanction Guidelines: Appendix 4B
  - Reliability and Security Technical Committee Update
  - 2020 ERO Enterprise Reliability Indicators Update
- Committee, Forum, and Group Reports

July 22 – MRC Informational Session

- Schedule and Preliminary Agenda Topics for the August 2020 Board, Board Committees, and MRC Meetings
- Overview of Policy Input Letter
  - E-ISAC Long-Term Strategic Plan
- NERC Bylaws Amendments

Upcoming Dates

- **July 15:** Policy input letter issued
- **August 5:** Written comments due on policy input topics and preliminary agenda topics
- **August 6:** Board and MRC agenda packages and policy input letter comments posted
- **August 13:** Board and MRC presentations posted

Questions and Answers

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Long-Term Strategic Plan Update

July 2020

RESILIENCY | RELIABILITY | SECURITY




1325 G Street NW
Suite 600
Washington, DC 20005
202-790-6000 | www.eisac.com

TLP:WHITE

Executive Summary

July 2020

Background

The Electricity Information Sharing and Analysis Center's (E-ISAC) Long-Term Strategic Plan has three primary focus areas—Engagement, Information Sharing, and Analysis—and embraces the following ongoing needs: review priorities under each focus area, ensure alignment between priorities, optimize resource allocation, and establish metrics to measure progress.

In 2019, the E-ISAC took steps to improve the efficiency of operations and reduce or eliminate certain lower-value activities. The E-ISAC strengthened its leadership and security operations and reorganized to align and optimize cyber and physical security teams as part of an integrated watch operations team. The E-ISAC also reorganized and enhanced its Portal posting and other publications to provide greater context and more information that is actionable. In addition, it created a performance management group to oversee the implementation of process improvements, technology, and metrics to improve the quality, timeliness, and value of information sharing, data management, and analysis.[1]

Near-Term Focus (2020–2021)

The E-ISAC's primary focus will be to improve the effectiveness and efficiency of current products, platforms, and services.[2] The E-ISAC will also sharpen its focus and execution regarding building and maintaining membership by demonstrating value through improved analysis, timely sharing of actionable information, collaboration with key government and strategic partners, and ensuring that E-ISAC operations are both effective and efficient.

The E-ISAC will adopt the following practices to guide resource allocation and investments while ensuring alignment with the three primary focus areas under the Strategic Plan: resource allocation and investment, engagement, and information sharing and analysis.

Longer-Term Focus (three to five years)

The E-ISAC will focus on providing additional value to members and other stakeholders in the following four key areas:

- Enhance the E-ISAC's analytical capabilities with both internal and partnership with third parties while ensuring these enhancements provide value to E-ISAC's members
- Work closely with the MEC working group, government, and industry partners to identify and share operational technology risks and risk mitigation strategies
- Enhance the E-ISAC's capability to better leverage classified and other critical threat and intelligence information (both nonpublic governmental and private sector) to provide timely and actionable information to the sector regarding security risks

[1] The E-ISAC's 2020 performance metrics are included as Attachment A.

[2] Attachment 2 is a listing of current E-ISAC products and services.

TLP:WHITE

- Conduct a detailed evaluation of the benefits, costs, governance and funding issues, and options that extend E-ISAC services and capabilities to support the downstream natural gas sector given cross-sector interdependencies

The E-ISAC will also continue to evaluate partnership opportunities with the commercial sector, other ISACs, and government-sponsored research and development organizations. The E-ISAC will also work closely with stakeholders and government partners to carefully evaluate the benefits, resource requirements, and potential challenges and risks associated with each of these initiatives. Finally, the E-ISAC will formulate appropriate program activities, budgets, and schedules through transparent resource planning and budget approval processes.

TLP:WHITE

E-ISAC Long-Term Strategic Plan Update
July 2020

Background

The Information Sharing and Analysis Center (ISAC) construct was authorized by a U.S. presidential directive issued in 1998 and is focused on engagement, information sharing, and analysis directly related to the protection of critical infrastructure. Due to a 1999 request by the U.S. secretary of energy that the North American Electric Reliability Corporation (NERC) serve as the ISAC for the electricity sector, NERC formed the E-ISAC.[3] The E-ISAC's fundamental purpose and mission is to support its members and other stakeholders to reduce cyber and physical security risk through quality analysis and timely sharing of actionable electricity industry security information.

The E-ISAC operates as a separate department within NERC. Electric load-serving entities fund the E-ISAC's operations and budget through payments to NERC for its annual assessments in North America. Participants in the Cybersecurity Risk Information Sharing Program (CRISP) support the program through separate contractual funding. The U.S. DOE developed CRISP, and the E-ISAC manages it.[4]

NERC's senior vice president and chief executive officer (CEO) of the E-ISAC is responsible for the day-to-day management of the E-ISAC. The Member Executive Committee (MEC) of the Electricity Subsector Coordinating Council (ESCC)[5] provides industry leadership to guide and support the E-ISAC, including strategy development and operational guidance. Current MEC membership includes executives from North American investor-owned, public power, and cooperative utilities. Members must be CEO-level executives, security executives, or subject matter experts employed or sponsored by an E-ISAC member organization. The NERC CEO is also a standing member of the MEC. NERC's Board of Trustees, through its Technology and Security Committee, provides corporate oversight of the E-ISAC, giving due consideration to MEC recommendations. This governance helps ensure that the E-ISAC remains focused on both the needs of its members and supporting NERC's role as the Electric Reliability Organization.

Development of Strategic Plan: Primary Focus Areas and Supporting Activities

In 2017, the E-ISAC—with guidance from the MEC, the NERC Board of Trustees (NERC Board), and various trade associations and stakeholder groups—developed a Strategic Plan to better define its mission and focus its resources towards helping to protect the electricity industry from escalating cyber and physical security risks. The Strategic Plan has three primary areas of focus: Engagement, Information Sharing, and Analysis. The Strategic Plan embraces the ongoing need to review priorities under each focus area, ensure alignment between priorities, optimize resource allocation, and establish metrics to measure progress. The

[3] NERC was designated by the Federal Energy Regulatory Commission as the Electric Reliability Organization under Section 215 of the Federal Power Act.

[4] Fees from security conferences and training events also provide additional, less significant sources of funding.

[5] The CEO-led ESCC serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for and respond to national-level disasters or threats to critical infrastructure. The ESCC focuses on actions and strategies that help protect the energy grid, prevent various threats from disrupting electricity service, and develop capabilities that help the sector quickly respond and recover when major incidents impact the grid.

TLP:WHITE

central underpinning of the Strategic Plan is for the E-ISAC to focus on providing timely and actionable information and analysis to industry regarding cyber and physical security threats and mitigation strategies; to advance this important objective, the Strategic Plan recognizes the critical interdependencies between the E-ISAC, industry, U.S. and Canadian government agencies, and other stakeholders.

The primary activities under each of the Strategic Plan focus areas are as follows:

Engagement

- Building and enriching the value of E-ISAC membership
- Strengthening trusted source relationships in both the private sector and government
- Enhancing engagement within the electricity industry in both the United States and Canada
- Continuing to improve and mature security exercises by expanding and increasing the diversity of participation, developing and refining scenarios to provide meaningful and practical learning opportunities

Information Sharing

- Increasing the quality and volume of information shared with E-ISAC from industry, government partners, and trusted third parties (including information from classified sources)
- Strengthening the E-ISAC's capabilities for information sharing
- Improving timeliness and actionable value of information shared from the E-ISAC to industry
- Implementing 24x7 watch operations that are effective, efficient, and responsive to member needs

Analysis

- Effective data collection and capture of new information sources
- Improving analytical tools and techniques
- Strengthening analytical capabilities through strategic relationships and hiring, developing, and retaining qualified staff

As part of managerial planning efforts for 2020–2021, management took feedback into account from the Board, MEC, members, and other stakeholders to assess progress to date, reconfirmed operating and strategic priorities, and identified both gaps and opportunities to further improve products and services and to provide greater value to members. The following is a summary of actions the E-ISAC will be undertaking to address these gaps and opportunities.

TLP:WHITE

Near-Term Focus (2020–2021)

The primary focus of the E-ISAC over the next two years will be improving the effectiveness and efficiency of current products, platforms, and services. The E-ISAC will also sharpen its focus and execution in building and maintaining membership by demonstrating value through improved analysis, timely sharing of actionable information, and collaboration with key government and strategic partners while ensuring that E-ISAC operations are both effective and efficient.

Key efforts will include the following:

- Demonstrating the value of information sharing by providing improved and more frequent information to E-ISAC members
- Engaging with both industry and government to ensure alignment on key priorities and supporting improvements to the effectiveness of E-ISAC products, services, and supporting platforms
- Focusing and reallocating resources to ensure proper support for these key priorities as appropriate

With these efforts in mind, the E-ISAC will adopt the following practices to guide resource allocation and investments while ensuring alignment with the three primary focus areas under the Strategic Plan:

- Fostering an inclusive, stable, productive, and effective work environment that attracts and maintains a diverse, talented, and action-oriented workforce
- Aggressively pursuing initiatives that increase operational effectiveness
- Prudently choosing resource intensive initiatives that expand the E-ISAC's scope and avoiding or deferring those that disperse the E-ISAC's focus
- Exploring opportunities to refine and increase the effectiveness and efficiency of operations[6]

With the support of industry, the MEC, and the NERC Board over the past two years, the E-ISAC has devoted considerable effort to improving the quality and value of analytical, engagement, management resources, and supporting systems to advance the objectives in the Strategic Plan. The National Infrastructure Advisory Council (NIAC) report emphasized that cyber and physical security threats that industry and other sectors are facing continue to escalate, threatening critical infrastructure, economic and government stability, and national security.[7] It has never been more important for the E-ISAC to maintain its focus on its core activities and continue to produce products and services to provide stakeholders with content that helps improve or inform their security posture, encouraging them to share information in turn. Member and stakeholder participation, including information sharing and feedback on products and services, continue to be critical to the E-ISAC's success and electric system security, reliability, and resilience.

[6] The E-ISAC has put in place performance metrics to help measure progress in achievement of Strategic Plan priorities. A copy of the current set of performance metrics is included as Attachment A. These metrics will continue to evolve and improve over time based on ongoing member feedback, actual results, and data availability.

[7] NIAC, Transforming the U.S. Cyber Threat Partnership Final Report, December 2019.

TLP:WHITE

Over the next two years, the E-ISAC's primary focus will be on strengthening and building relationships across industry and government by demonstrating the value of products, services, and supporting platforms to increase information sharing and to help stakeholders reduce risk and improve their security posture.

Engagement

Successful implementation of the Strategic Plan requires that members know of E-ISAC products and capabilities and that they have opportunities to engage, interact, and provide input. Above all, members and stakeholders must recognize the value of information sharing and view the content, analysis, and context offered in E-ISAC products and services as instrumental pieces of the larger effort to reduce risk to the electricity industry.

The E-ISAC's engagement efforts will focus on communicating this value and encouraging the collaborative exchange of information, ideas, best practices, and insights related to understanding, remediating, and mitigating security risks. The E-ISAC focuses its engagement efforts on increasing industry participation and feedback regarding E-ISAC information sharing programs, capabilities, products, and services.

Areas of near-term focus for improvement of engagement activities include the following:

- **Expanding and Diversifying Membership:** Current membership represents 30% of NERC registered entities (covering approximately 80% of the electric meters in the United States) and 70% of Canada's electric utilities. Engagement efforts will focus on identifying, targeting, and engaging with underrepresented segments of the industry to ensure that all stakeholders, at varying sizes and geographic locations, are knowledgeable about the benefits of E-ISAC membership to reduce risk and improve their organizations' overall security posture.
- **Developing a More Formal Onboarding Process:** The E-ISAC is working on enhancing stakeholder onboarding processes and engagements through the development of a more mature onboarding process.
- **Leveraging the E-ISAC's Customer Relationship Management (CRM) Platform:** Fully implementing and maximizing the use of the E-ISAC's new CRM platform will increase and diversify membership and improve member services by obtaining and tracking member feedback, including through use of platform supported member surveys.
- **Explore Opportunities to Increase Efficiency of Security Exercises and Conferences:** The E-ISAC will explore opportunities to refine and increase the efficiency of supporting activities and resource allocations for GridEx and GridSecCon, both of which have experienced significant increases in participation and required increased resource support over the past four years. The E-ISAC will solicit competitive proposals for key activities supporting both GridEx and GridSecCon as well as evaluating partnering opportunities.

TLP:WHITE

Information Sharing[8]

Members voluntarily sharing security threat, vulnerability, and event/incident information is critical to achieving the goals in the Strategic Plan. Reliable and timely information sharing enables rich and highly contextual understanding of and the mitigation of security risks.

While members have made progress in increasing information sharing, considerable work remains, including reducing real and perceived barriers to information sharing. As of the end of 2019, the E-ISAC had over 1,200 active member organizations. However, only 10% of those organizations voluntarily shared information in 2019, and only 9 organizations provided more than 10 total unique shares last year. Investor-owned utilities provided over 65% of voluntary shares in the second half of 2019 with public power utilities providing the next most at just under 11%. The top 10 sharing organizations provided almost 50% of all shares. This reflects a very concentrated set of members that participate actively and regularly in voluntary information sharing. In 2019, the greatest sharing came almost exclusively from investor-owned utilities, 1 large public provincial Canadian utility with over 5,000 employees, and 1 Reliability Coordinator.

Willingness to share information varies across the industry, and barriers include the time and effort required to share information.[9] Currently, if a member wants to share security information, they have several choices: they can login to the E-ISAC Portal and manually enter and submit a post; they can email a bulk incident log report to E-ISAC; or they can contact the E-ISAC support team via phone or email. See the following for findings on each:

- **Portal Reports:** members can complete these on a timely basis, but this requires manual and often duplicative data entry (i.e., the member's security team staff has already captured the information, often manually, in their own tracking systems and then have to re-enter the data in the E-ISAC system).
- **Bulk Incident Log Reports:** only a handful of members use this method for physical security incidents, it provides some efficiency, but this occurs on a monthly basis and therefore is not as timely (although it assists in performing trending analyses).
- **Phone Calls and E-mails Reports:** these are inefficient and less frequent. In addition, many smaller organizations do not have the staff or technology to monitor and track this type of information in the first place, much less share it with E-ISAC.

The E-ISAC's near-term focus for improving information sharing includes enhancing the Portal to make it easier for members to share, manage, and find information; increasing the span, quality, and volume of voluntary shares from members; improving and expanding automated information sharing; and improving the security watch operations availability and capabilities.

[8] Information sharing includes both information sharing by members and partners with the E-ISAC as well as sharing of information by the E-ISAC with members and partners. Both activities are also closely aligned with and impact engagement and analysis activities.

[9] Organizational culture may also impact willingness to engage in voluntarily sharing information with third parties regarding risks or vulnerability due to uncertainties regarding benefits, fear over potential impacts on the corporate reputation, regulatory/compliance risk, or perceptions of corporate, departmental, individual and managerial capability or performance.

TLP:WHITE

Enhancing the Information Sharing Portal

The E-ISAC will implement the following changes to the Portal:

- Driven by the 2019 MEC working group guidance, the E-ISAC will expand available structured information fields driven by sub-type events and incidents for both physical and cyber voluntary share postings.
- The E-ISAC will redesign information-sharing account groups into more granular and discernable options.
- Driven by efficiency, internal control needs, and leading ISAC best practices, the E-ISAC will implement a designated approving official (DAO) role for each member and partner organization. The DAO role will allow self-service management of an organization's Portal users and periodic certification of existing users and organization profile information.
- The E-ISAC will enhance member ability to manage and search information, including Portal postings.

Increasing the Span, Quality, and Volume of Voluntary Shares from Members

Voluntary and timely information sharing of quality information by members provides critical additional context as well as a more accurate view of real-time security incidents that are occurring within industry. This information directly enhances the E-ISAC's ability to provide more accurate information and trend analysis back to industry.

In 2019, members shared significantly more physical security information than previous years.[10] Two key drivers of this success were increased engagement with individual members through an industry supported physical security analyst outreach program and the implementation of a bulk information sharing process. Bulk information sharing means sharing information about many incidents all at once with a method that reduces the sharing burden on individual members. This voluntary process tailors to the needs of individual members and can include sharing monthly summaries of incidents, transmission of security logs, or any other sharing method (e.g., email) that is beneficial for the member.

The E-ISAC also manages a Physical Security Advisory Group (PSAG)—a group of electric industry physical security subject matter experts that assist the E-ISAC in advising electricity industry participants and governmental agencies on threat mitigation strategies, incident prevention and response, training, emerging security technologies, and other relevant topics to enhance electric industry physical security and reliability. The E-ISAC's physical security team will work closely with PSAG to obtain their guidance in the development and refinement of physical security products and services that bring value to the E-ISAC's members as well as ways to increase member physical security information sharing.

[10] In 2019, following an aggressive push to increase physical security information sharing by directly reaching out to members, conducting analyst-to-analyst exchanges, and introducing the ability to share incidents in "bulk," physical secure incident sharing increased to 1384 incidents shared from 207 in 2018.

TLP:WHITE

The E-ISAC will also explore the creation of an industry-supported cyber security advisory group as a forum for engagement and collaboration regarding emerging cyber security risks, best practices, and feedback on E-ISAC cyber security related products and services as well as ways to increase member cyber security information sharing.[11] The E-ISAC will also work with the MEC working group and trade associations to continue to engage members in an effort to educate members regarding the benefits of information sharing and drive further increases in information sharing.

Improving and Expanding Automated Information Sharing

Steps to improve and expand automated information sharing will include the following:

- **Implementing an automated information sharing pilot program in 2020 for a limited set of willing and capable members for voluntary information sharing in a bidirectional fashion between external parties' applications and E-ISAC applications:** The pilot will explore the feasibility of creating bidirectional machine-to-machine data exchanges between E-ISAC and members. This will directly address the time-and-cost barrier to information sharing by reducing information sharing latency and eliminating duplicative data entry. The 2020 pilot approach is iterative, starting with a small set of participants and a practical set(s) of data to explore the costs/benefits and ongoing feasibility of possible expansion of the program in 2021.

- **Conducting a cost-benefit analysis of expanding the automated sharing to include additional types of data and information beyond that which is shared via voluntary information shares:** This may include raw network activity data (similar to CRISP) and/or new types of operational technology data and/or physical incident data. Note that this is only after sufficient due diligence accompanies the pragmatism of such an endeavor and if the lack of a sufficient alternative option(s) exist(s).

- **Where practical and cost-effective piloting and adopting various open source analysis support tools to achieve greater information gathering and analysis efficiency with a broader swath of staff:** These tools drive "smart" alerting and rapid information harvesting by placing automated, parameter-driven targeted searches into the hands of all E-ISAC analysts.

Maturing Security Watch Operations

To support E-ISAC information sharing and response capabilities, the E-ISAC recently established on-duty 24x5 watch operations and will be moving to 24x7 on-duty watch operations by no later than the third quarter of 2020. The Security Operations team is transforming towards a unified "team of teams" with common proactive and reactive goals, culture, and capabilities. It will achieve operational excellence through proactive, quality product delivery, and reactive around-the-clock incident-management services delivery. Security Operations also delivers a class of incident response communications and sharing, including All-Points Bulletins, Critical Broadcast Program calls, ESCC Playbook calls, and other government-sponsored and industry-supported incident response communications. While Security Watch Operations is

[11] This will including leveraging work undertaken by and participation in NERC's industry supported Critical Infrastructure Protection Committee and the more recently formed Reliability and Security Technical Committee.

TLP:WHITE

just one of several information sharing channels,[12] it plays an important role in communicating the value of E-ISAC membership and advancing voluntary information sharing by members.

Improving Government Collaboration and Access to Classified Information

The E-ISAC collaborates with the U.S. and Canadian intelligence agencies to do the following:

- Advocate for timely, actionable, and relevant threat information suitable for the electricity industry to help stakeholders mitigate risks
- Represent the electricity industry in both unclassified and classified analysis, discussions, and initiatives on physical and cyber threats to critical infrastructure
- Educate and provide awareness on the technical, business, and cultural aspects of the electricity industry to support governmental authorities and capabilities to both inform and protect industry

The E-SAC's physical security team is also strengthening its working relationship with the Royal Canadian Mounted Police. The team is coauthoring a white paper on wind farm security risks, exploring analyst exchange opportunities, and is conducting Royal Canadian Mounted Police training on the physical security design basis threat methodology. This team also established a relationship with the Canadian National Counterterrorism Center to further advance physical security information sharing, education, and training. The E-ISAC anticipates ongoing collaboration with these entities over the planning period.

The E-ISAC recently entered into a memorandum of understanding with DOE. The primary objectives of this agreement are to do the following:

- Define the relationship between DOE and the E-ISAC as it relates to their respective roles in enhancing the electricity industry's efforts to prepare for and respond to cyber and physical security threats, vulnerabilities, and incidents
- Provide a general framework for cooperation between the parties regarding information sharing and analysis and cyber and physical security incident coordination and response
- Articulate expectations for the exchange of relevant information in a timely, reliable, and effective manner in response to cyber and physical security threats, vulnerabilities, and incidents

Management is working closely with the DOE to operationalize this memorandum of understanding, including defining deliverables, accountabilities, and schedules. The E-ISAC will also work closely with the ESCC, industry, and applicable government agencies to define how the E-ISAC can best support implementation of the recommendations of the NIAC and Cyber Solarium Commission as well as to support Pathfinder initiatives within the sector.

While the E-ISAC has established some collaboration with federal partners at the classified level, the E-ISAC must continue to expand its role in supporting classified information sharing between government and

[12] Other information sharing channels include voluntary and mandatory member/partner shares including news, bulletins, threat indicator sharing, other relevant, timely and useful data set sharing, finished reporting and bulk data sharing, a variety of government, industry and member briefings, exercises and conferences where information is shared through presentations, and other oral communications.

TLP:WHITE

industry. As referenced in the recent NIAC and other national level reports, there is an increasing need for public-private partnerships and information sharing in classified as well as unclassified venues. In addition to supporting the NIAC, Cyber Solarium, and Pathfinder initiatives, near-term and related E-ISAC activities involving classified arenas include working to do the following:

- Improve E-ISAC access to classified information and threat briefings to further develop and steer programs such as CRISP and E-ISAC threat information sharing to industry
- Increase meaningful classified threat briefings to industry
- Strengthen classified collaboration with DOE, DHS, and other government agencies to enhance sharing emerging security risks information with the electricity industry
- Provide electricity fundamentals training to government partners in both classified and unclassified settings to both educate and provide awareness of the electricity industry and related cyber and physical security issues with the goal of helping to better inform their threat and intelligence analysis

Analysis

Providing timely, actionable, and value-added analysis to members is critical to the E-ISAC's success. The E-ISAC uses four primary sources of information to accomplish this: information provided by CRISP participants,[13] voluntary member shares, information from partners, and open-source information. E-ISAC staff takes all of these inputs, conducts filtering and analysis of this information, and produces information products, including bulletins (cyber or physical), documents (white papers, reports, etc.), filtered news, and filtered indicators-of-compromise lists. In addition, as part of the CRISP program, participating members receive unclassified briefings and reports, and the E-ISAC Portal provides anonymized information with members and trusted partners subject to the terms of confidentiality agreements. On a less frequent but often more critical basis, the E-ISAC also facilitates and/or participates in classified information discussions and exchanges of information involving appropriately cleared personnel across government and industry.

The E-ISAC's near-term analysis focus will be in the following four areas:

- **Increasing the Frequency of Valuable, In-depth Analysis:** This includes improving business processes, deploying technology to drive greater efficiency, and freeing up resources to support the development and sharing of more valuable analytical products. Leveraging additional quantitative data analysis techniques for identifying observed security patterns and trends across the industry is also important.
- **Improving the Quality and Timeliness of Reports:** The E-ISAC will focus on the quality, relevancy, and timeliness of information sharing in general as they apply to reporting (the right reporting on the right subjects with the right quality at the right times). The E-ISAC will drive progress through focus on the design and execution of supporting quality control processes, such as inbound and outbound product quality assessments.

[13] The Pacific Northwest National Laboratory, within the strict confines of the CRISP structure where it is subject to detailed data handling and other contractual protections, analyzes information provided by CRISP participants. The E-ISAC has access to CRISP information for purposes of conducting its own analysis for the benefit of CRISP participants. The E-ISAC uses unclassified information derived from CRISP to conduct additional more board-based analysis of sector threats.

TLP:WHITE

- **Operationalizing Agreements:** The E-ISAC recently entered into collaboration agreements with the Independent Electricity System Operator, the Multi-State ISAC (MS-ISAC), and the Downstream Natural Gas ISAC. The objectives of each of these agreements is to strengthen information sharing to further enhance analytical products that can be shared with each of these organizations, their members, and other trusted stakeholders. The parties to operationalize the objectives contained in these agreements have designated lead representatives. The principles behind this focus on communication, mutual commitment to defined goals, and shared principles governing dissemination of threat information. The E-ISAC has developed monthly plans that identify key activities and milestones associated with each of the major undertakings. Each month, the E-ISAC reviews these plans and at least annually will conduct an overall evaluation of the progress achieved in connection with each collaboration agreement. Management will also explore similar collaboration initiatives with other strategic partners after assessing the potential benefits and supporting resource requirements.

- **Expanding CRISP Participation and Driving CRISP Data Enrichment and Analysis:** Participation in CRISP has grown significantly in partnership with DOE, which continues to provide significant institutional and financial support for the program, including specific initiatives directed at increasing participation. The E-ISAC is also supporting initiatives to streamline program governance and drive greater program value through data enrichment and analysis. An operational technology pilot is in the evaluation and planning stages; the objective of this pilot is to explore the ability to view and analyze security risks associated operational and control systems technologies and advance participant and stakeholder understanding of the threat landscape facing the utility industry. Additionally, CRISP is in the midst of a Syslog pilot that focuses on collecting and analyzing two new data types to the program: email headers and inbound secure socket layer data. Both of these datasets inform more robust analysis of CRISP data in general and provide insight into anomalous and/or malicious activity affecting the CRISP community. The Syslog pilot will enter operations in 2021. Finally, CRISP is exploring new data collection capabilities through both hardware and software and will begin piloting these in 2021.

In addition, while all registered users of the E-ISAC Portal have access to postings of unclassified information derived from CRISP, there are practical financial and administrative limitations on the ability of smaller utilities to participate directly given the current cost and complexity of the program. The E-ISAC is working with trade associations—the American Public Power Association and National Rural Cooperative Association—and DOE to explore ways to further leverage CRISP and/or similar technologies to benefit small public power companies.

Many municipal and public power utilities outsource their security operations to the MS-ISAC, which is funded by the Department of Homeland Security and attractive to public power organizations with smaller security monitoring budgets. The MS-ISAC offers a sensor program through which it collects and analyzes network security risks for these smaller participating utilities. The E-ISAC is working with the MS-ISAC to explore opportunities to leverage this sensor information further with other E-ISAC data sources, including CRISP, to allow the MS-ISAC to enhance the services provided to these smaller government owned utilities.

TLP:WHITE

The success of the E-ISAC's analysis objectives and related strategic partnership initiatives is closely tied to the development and deployment of technology to leverage data and information sharing with these entities. This is particularly true with respect to improving and expanding data analytics and associated threat activity insights by combining data from these entities with other available data sources. As noted above, the planned CRISP operating technology pilot will focus on assessing the viability of looking across information and operating technology data to better identify anomalous and malicious activity that affects electricity subsector industry control systems. From a technology perspective, E-ISAC staff is implementing a new data platform. This data platform will increase the speed by which E-ISAC analysts can access, correlate, analyze, and visualize information from across many different data sources, such as open source information, voluntary shares, case tickets, new partner data, and the CRISP data sets. The E-ISAC operations team will use these capabilities to provide more targeted, timely, and enriched information to members. In addition, as mentioned, an automated information sharing pilot is scheduled for 2020 and is aimed at reducing one of the information sharing barriers (cost and time to share) by eliminating redundant data entry and reducing data latency for those that chose to participate. This will facilitate increased member information sharing and security awareness among Portal information sharing groups as well as serve as input into E-ISAC analytical products. The E-ISAC will also leverage enhanced case management and workflow to increase the effectiveness of timely and quality production of information products for the E-ISAC's members. Finally, the E-ISAC will use its CRM system to better track, target, and provide more meaningful and consistent interaction and messaging with E-ISAC partners and members. All of these initiatives will enhance the E-ISAC's ability to provide better service to its members.

Longer-Term Strategic and Resource Planning Consideration (3–5 Years)

As the E-ISAC looks at the longer-term time horizon, it is considering several initiatives to provide additional value to its members and other stakeholders, including the following:

- Enhancing the E-ISAC's analytical capabilities, both internal and in partnership with third parties, while ensuring these enhancements provide value to E-ISAC members
- Working closely with the MEC working group, government, and industry partners to identify and share operational technology risks and risk mitigation strategies
- Enhancing the E-ISAC's capability to better leverage classified and other critical threat and intelligence information (both nonpublic governmental and private sector) to provide timely and actionable information to the sector regarding security risks
- Conducting a detailed evaluation of the benefits, costs, governance and funding issues, and options extending E-ISAC services and capabilities to support the downstream natural gas sector, given cross-sector interdependencies

In addition, the E-ISAC will continue to evaluate partnership opportunities with the commercial sector, other ISACs, and government sponsored research and development organizations. The E-ISAC will also work closely with stakeholders and government partners to carefully evaluate the benefits, resource requirements, and potential challenges and risks associated with each of these initiatives as well as in the formulation of appropriate program activities, budgets, and schedules through transparent resource planning and budget approval processes.

TLP:WHITE

Attachment 1

2020 Performance Metrics		
Engagement		
Percent increase in prospective member organizations engaged	Percent increase in diversity of types of member organizations participating in Industry Engagement Program and E-ISAC led workshops	Percent increase in cross-sector participation in GridEx
Percent increase in prospective member organizations that sign up to use the E-ISAC portal.	Percent increase in Canadian member organizations	Percent increase in state government participation in GridEx
Frequency of member user interactions by channel	Canadian Electricity Association support of 2021 budget	Quality and usefulness of CRM tool and data: actual results compared to business case assumptions
Elapsed time since last member interaction (e.g., share or contact)	Percent increase in GridEx participation	
Analysis		
Percent increase of content enriched by E-ISAC analysts	Percent increase in joint analytical products with partners	E-ISAC Data Platform project implementation variance from plan
Unclassified Threat Workshop content survey results (relevant, timely, unique, actionable)		
Information Sharing		
Member Portal Sharing: Percent increase in number of portal posts by member organizations	**Member Information Sharing:** Volume of member organization information sharing within predefined peer groups	**Implementation of Portal Enhancements Per Approved Project Plan**
Total Information Shares: Percent increase in number of information shares by source, channel, and event type	**Member Information Sharing:** Percent increase in quality and unique value-add information received from member organizations	**Security Watch Operations Coverage:** • On Duty: Core Hours Head Count • On Call: Off Hours Head Count • On Duty: Off Hours Head Count
Partner Information Sharing: Percent increase in volume of information shares received from partner organizations Percent increase in quality of information shares received from partner organizations	**Percent Increase in Targeted Feedback from Members and Partners**	**Security Watch Operations Sharing:** Indicators of compromise (IOC) loaded into external sharing platform
Staffing and Attrition		
Annual employee attrition rate	Total staff and period over period net change	

TLP:WHITE

Attachment 2
List of Products and Services

Products	Description	Audience
Monthly Report	A high-level, summary report that includes monthly trends and analysis that industry members can use to help inform products for industry leadership	All asset owner and operator (AOO) members
Annual Report	An executive-level overview of E-ISAC accomplishments and future trends covering a range of security topics and E-ISAC programs	AOO senior management and CEOs
E-ISAC Brochure	A high-level overview of the E-ISAC offerings and the benefits of becoming a member of the E-ISAC	Prospective or new members and partners
White Papers (Xenotime, Ukraine, Ransomware)	A deep dive analysis into significant or highly publicized events and trends in the industry	AOO cyber and physical analysts
Bulletins, Portal Postings, and Notifications	Timely, informative portal postings relaying information on cyber or physical events as well as national events/comments on media coverage of issues pertaining to the industry	AOO cyber and physical analysts
Services (Workshops, Webinars, Working Groups, Platforms, Conferences, and Exercises)	**Description**	**Audience**
Portal	Provides a central repository for the bidirectional sharing of information between E-ISAC members, partners, and staff	All members and partners with Portal access
Cyber Automated Information Sharing System (CAISS)—IOC feeds	Provides participating members with a daily, automated feed of indicators of compromise based on the STIX/TAXII protocol	Participating AOO members
CAISS—threat platform community	Provides participating members with the ability to share and collaborate on cyber security items via a common third party tool	Participating AOO members

TLP:WHITE

Services (Workshops, Webinars, Working Groups, Platforms, Conferences, and Exercises)	Description	Audience
Monthly Briefing Series (Webinar)	A monthly webinar hosted by the E-ISAC featuring cyber and physical security updates as well as news and trends from partners, including government and cross-sector partners; recordings are posted to the Portal and content is incorporated into the Monthly Report	All AOO members
GridSecCon	Annual conference cohosted by NERC, the E-ISAC, and a rotation of NERC Regional Entities; this brings together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, training, and lessons learned	All members and partners
GridEx	Held every other year, to exercise utilities' crisis response and recovery procedures, improve information sharing during a crisis, gather lessons learned, and engage senior leadership	All members and partners
Cybersecurity Risk Information Sharing Program (CRISP)	CRISP leverages all-source cyber threat intelligence and government-informed reporting to detect threats to North American electricity companies. CRISP is a private-public collaboration coordinated by the E-ISAC between the U.S. DOE and North America's electricity industry. All E-ISAC members benefit from the information gathered regardless of CRISP membership status.	CRISP members
CRISP Workshops	The E-ISAC hosts CRISP workshops twice a year for CRISP participants to discuss threats and to provide an opportunity for participants to network, collaborate, and gain a thorough understanding of the program and identify key areas of enhancements to capabilities from a technical and analytical perspective. This includes a classified briefing for cleared participants.	CRISP members
Industry Engagement Program	A three-day program for small groups of industry analysts to gather at the E-ISAC D.C. office to increase awareness of E-ISAC capabilities,	Open to industry members, with a focus on analysts or those

TLP:WHITE

Services (Workshops, Webinars, Working Groups, Platforms, Conferences, and Exercises)	Description	Audience
	products, and services and to share best practices and lessons learned with industry colleagues	with information sharing responsibilities
Threat Workshops (Unclassified)	An unclassified workshop hosted by the E-ISAC, focused on facilitating dialogue between industry members and government security specialists about specific grid cyber and physical threats	AOO cyber and physical analysts
Design Basis Threat Implementation Workshop	Designed to teach participants how to use design basis threat methodology to enhance the physical security of assets	AOO security personnel and analysts
Electricity Subsector Coordinating Council Working Groups	Support and provide subject matter expertise and leadership to help inform ESCC working groups and activities. This includes participation and coordination on ESCC meetings, ESCC working groups, Senior Executive Working Group, weekly government-industry call, and the MEC.	AOO executives and CEOs
Government and Cross-Sector Coordination	Support and provide leadership and technical expertise on security and resilience for government and cross-sector efforts. This includes participation and coordination with the National Council of ISACs, the leading critical infrastructure cross sector community as well as management of international, federal, state, provincial, and local government partners.	All members and partners
Physical Security Advisory Group (PSAG)	An E-ISAC led group that provides expertise to advise the industry on the threat mitigation strategy to enhance physical security and reliability. The group is comprised of over 20 physical security leaders from across industry security, government, and other partners.	AOO physical security members
Critical Broadcast Program	E-ISAC facilitated call to rapidly convene large groups of industry members to share information about imminent/emerging security issues that would operationally or otherwise impact industry.	All AOO members, especially managers and executives

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Jack Cashin, Director, Policy Analysis and Reliability Standards, American Public Power Association
John Di Stasio, President, Large Public Power Council
John Twitty, Executive Director, Transmission Access Policy Study Group

DATE: August 5, 2020

SUBJECT: Response to Request for Policy Input to NERC Board of Trustees

---

The American Public Power Association, Large Public Power Council, and Transmission Access Policy Study Group concur with the Policy Input submitted today by the State/Municipal and Transmission Dependent Utility Sectors of the Member Representatives Committee, in response to NERC Board Chair Roy Thilly's July15, 2020 letter requesting policy input in advance of the August 2020 NERC Board of Trustees meetings.

NERC Board of Trustees Policy Input – Canadian Electricity Association

The Canadian Electricity Association ("CEA") appreciates this opportunity to provide further policy input to the NERC Member Representatives Committee ("MRC") and Board of Trustees ("Board").

Summary of Key Points:

- CEA agrees with the overall objectives of the strategic plan.
- The E-ISAC should continue to efforts to leverage capabilities already available from other agencies or partners, and to optimize and further action existing partnerships.
- It is important that activities to achieve the strategic plan are balanced with fiscal responsibilities and ensuring cost-efficient operations. There should be value for all stakeholders.
- The E-ISAC should ensure actions are within their mandate and scope of responsibility, and to also recognize that different jurisdictions may identify and approach threats, and determine actions to respond to those threats, differently.
- The E-ISAC should ensure that the focus areas of the strategic plan can be appropriately implemented in a Canadian context. It should focus its actions on complementing, rather than duplicating, the information sharing efforts of Canadian and American government security partners through offering a unique North American viewpoint and cross-border situational awareness perspective.

1. Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?

CEA appreciates the work undertaken to update the strategic plan, including the ongoing consultation with E-ISAC stakeholders and users.

Over the past few years, CEA and its members have urged NERC to improve the value proposition of the E-ISAC for all stakeholders, including Canadians, while also ensuring cost-effective and efficient operations. In this context, and with the underlying goal of helping to ensure the security of the Bulk Power System, the overarching focus areas of 'Engagement, Information Sharing, and Analysis' for the strategic plan seem appropriate and welcome.

Regarding the short-term focus areas, CEA agrees with the objectives to improve the effectiveness and efficiency of current products, platforms, and services. CEA also agrees with the focus of demonstrating value through improved services, more timely and actionable information sharing, and collaboration with key partners.

Regarding collaboration with key partners, CEA encourages NERC and the E-ISAC to continue efforts to leverage capabilities already available from other agencies or partners, such as the Canadian Centre for Cyber Security, and to optimize and further action existing partnerships. This also includes continuing to pursue, where relevant, joint information sharing partnerships with other critical infrastructure sector ISACs.

Regarding the longer-term objectives, CEA agrees that the focus must remain on providing unique value to E-ISAC members and to the electricity security community at large, including through offering a North American perspective of the pressing security issues facing the electricity sector.

2. Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members?

While CEA agrees with the overall objectives of the strategic plan, it is important that activities to achieve the plan are balanced with fiscal responsibilities and ensuring cost-efficient operations. In a presentation to the E-ISAC Members Executive Committee on July 21st, it was noted that there are projected budget increases for the E-ISAC in 2022 and 2023. Further, the strategic plan represents a broad agenda in terms of impact and ambition. In terms of resource constraints for both the E-ISAC and industry, and needing to ensure alignment between activities, pursuing a large number of initiatives concurrently (even during the COVID-19 pandemic), may offer execution challenges, including for electricity stakeholders to participate fully in the different initiatives.

As such, CEA reiterates the need to ensure that there is corresponding value for all stakeholders, for the E-ISAC to continue to seek appropriate ways to reduce costs, and for the focus to remain on the highest value activities. This includes the need for:

- ongoing review of activities and initiatives to ensure that resources are appropriately directed to achieve value;
- prioritizing the activities that bring the highest value, and eliminating or modifying ones that do not;
- leveraging existing threat sharing and analysis infrastructure;
- optimizing resources;
- continuing to promote and strengthen information sharing among both new and existing members;
- ensuring alignment between activities; and
- avoiding duplication of efforts.

As the strategic plan is implemented, care must be taken to continue to ensure that the E-ISAC's focus and actions are within its mandates and scopes of responsibility, especially as they relate to avoiding potential overlaps with what is within the jurisdictions of Canadian and American governments, and their respective intelligence agencies. NERC and the E-ISAC should also remain focused on the threats that most affect the North American Bulk Power System at large, recognizing that while all of the E-ISAC's stakeholders hold reliability and security of the grid as a top priority, different jurisdictions may identify, approach threats, and determine actions to respond to those threats, differently depending on their unique contexts.

As the strategic plan enters its implementation phase, CEA strongly encourages NERC and the E-ISAC to continue its positive engagement with stakeholders, and to continue to find ways to enable constructive and efficient feedback between E-ISAC participants and leadership on an ongoing basis. This includes leveraging the membership of the E-ISAC MEC, and providing regular, planned updates on progress and issues.

This can help ensure that the full value of the E-ISAC, and the goals of the strategic plan, can be realized for all.

In support of this goal, CEA recommends that the E-ISAC work with Canadian stakeholders to ensure that the focus areas of the strategic can be appropriately implemented in a Canadian context, in a way that recognizes unique Canadian jurisdictional and policy realities. This would help to ensure the full value of the E-ISAC can be realized for entities in both the U.S. and in Canada.

Ensuring that the strategic plan is applicable in a fully North American context can increase the value proposition for the E-ISAC for all stakeholders, through further enabling the E-ISAC to offer a unique North American perspective of the evolving security challenges faced by the electricity sector. This can happen though increased timely and actionable information sharing between E-ISAC members and partners from both Canada and the U.S., which can then serve to assist the E-ISAC in providing North American wide situational awareness and analysis. Further, it can assist with optimized and deepened collaboration between government, industry, and other and security partners on both sides of the border.

CEA and other Canadian stakeholders would look forward to continuing to work with NERC and the E-ISAC in support of these objectives.

CEA thanks the Board for considering these comments. CEA and its members look forward to continuing the discussion going forward.

Dated: August 5th, 2020

Contact:
Francis Bradley
President & CEO
Canadian Electricity Association
Bradley@electricity.ca

Edison Electric INSTITUTE

Power by Association

Policy Input for the NERC Board of Trustees
Provided by the Edison Electric Institute
August 5, 2020

On behalf of our member companies, the Edison Electric Institute (EEI) appreciates the opportunity to provide the following policy input for the NERC Board to review in advance of the August 19-20, 2020, meetings. EEI perspectives on bulk-power system (BPS) reliability are formed by our CEO Policy Committee on Reliability, Security, and Business Continuity and the Reliability Executive Advisory Committee with the support of the Reliability Committee.

In the July 15, 2020 policy input letter, NERC Board of Trustees Chair, Roy Thilly, seeks input on the E-ISAC Strategic Plan and NERC Bylaws. EEI offers the following input.

E-ISAC Strategic Plan

- EEI generally supports the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan.
- Regarding E-ISAC near term focus, EEI agrees that with the statement (p. 6) that, "[i]t has never been more important for the E-ISAC to maintain its focus on its core activities and continue to produce products and services to provide stakeholders with content that helps improve or inform their security posture, encouraging them to share information in turn."
- In the Near-Term Focus section (p. 6), E-ISAC states that it will adopt the following practice: "Prudently choosing resource intensive initiatives that expand the E-ISAC's scope and avoiding or deferring those that disperse the E-ISAC's focus."
    - This statement could be read to indicate an interest in expanding or materially changing the ***scope*** of the E-ISAC, although EEI acknowledges that this was likely not the intent. If though, expanding the scope was the intent, this statement can be read to be inconsistent with the E-ISAC charter and potentially neglects the important role of industry stakeholders. We recommend clarifying this statement.
- In the Engagement section (p. 7) E-ISAC recognizes "the value of information sharing" and "communicating this value." It is essential that the E-ISAC also

focuses on ***delivering*** measurable value to participating electric utilities, and we recommend adding language to that effect.

- As the E-ISAC contemplates (p. 7) "Leveraging the E-ISAC's Customer Relationship Management (CRM) Platform," it is important that value to participating electric utilities drive the discussion, activities and efforts.
- The E-ISAC will (p. 7) explore opportunities to refine and increase the efficiency of supporting activities and resource allocations for GridEx and GridSecCon. E-ISAC staff investments should be commensurate with the goals of the E-ISAC. There is no shortage of conferences or seminars that address areas of interest to electric utilities, so any action taken by E-ISAC should avoid duplication and be consistent with the discrete incremental activities of the E-ISAC in hosting such events.
- With respect to Automated Information Sharing, if would be helpful if the E-ISAC provided additional information on the means and manners that are available to limit regulatory liability associated with such sharing. Additionally, it is important to ensure the information sharing program does not duplicate efforts underway at DOE, including CATT and COYOTE.
- Additional detail is requested about the CRISP OT Pilot. Additionally, EEI recommends that the E-ISAC collaborate with industry users in the development of requirements for this effort.
- Concerning consideration for extending E-ISAC services and capabilities to support downstream Natural Gas ISAC, priority must remain on the electric sector. There should be clear, quantifiable value to electric sector operators when contemplating engagement with other entities, including the following considerations:
    - How will E-ISAC manage data collection that does not directly affect BPS security or cannot be managed within the constraints of limited resources—even if the pipeline companies pay for that service;
    - How will E-ISAC account for the increase in information to a point where communications are ineffective due to volume;
    - Are the natural gas attack vectors shared by the BPS; and
    - Will E-ISAC need to develop additional expertise to supervise security of the downstream natural gas sector?

NERC Bylaws

- EEI supports NERC's proposed revisions to the Bylaws and appreciates NERC's outreach with industry and consideration of industry feedback.

Thank you for the opportunity to provide policy input.

Sector 8 Policy Input for the NERC Board of Trustees & Member Representatives Committee

August 19-20, 2020 Meetings

ELCON, on behalf of Large End-Use Consumers, submits the following policy input for the consideration of NERC's Board of Trustees (BOT) and the Member Representatives Committee (MRC). It responds to BOT Chairman Roy Thilly's July 15, 2020 letter to Jennifer Sterling, chair of the MRC.

SUMMARY

Large Consumers (Sector 8) are pleased with the development of the Electricity Information Sharing and Analysis Center (E-ISAC) and support the base elements of its Long-Term Strategic Plan.

1. **Strategic and Operational Focus Areas of the E-ISAC strategic plan.** E-ISAC's mission is right on point with a sound cybersecurity policy strategy; promote voluntary, risk-informed decisions by the private sector. E-ISAC's services and products could be better tailored to resource-constrained stakeholders whose core businesses do not include selling power. This includes better contextualization of risk mitigation strategies and data analytics, along with more expeditious transfer of classified information. Expanded coordination with other ISACs whose industries affect Large Consumers, such as ONG-ISAC and IT-ISAC, would be welcomed. E-ISAC should also employ expanded cost-benefit analysis.
2. **Recommendations for other E-ISAC Areas.** NERC should work to alleviate concerns that inhibit E-ISAC membership recruitment. NERC and E-ISAC should endeavor to codify E-ISAC's functional separation from NERC's compliance monitoring and enforcement arm as integral to the achievement of its strategic objectives.

Strategic and Operational Focus Areas

Cybersecurity policy in the electricity industry is most effective and economical when it promotes voluntary, risk-informed decisions by the private sector. E-ISAC's mission is well aligned with this. The Plan's three primary focus areas – Engagement, Information Sharing, and Analysis – are on-point with E-ISAC's mission. Large Consumers seek to make E-ISAC's fulfill its mission subject to reasonable budgetary constraints. Should E-ISAC's mission expand beyond this scope, Large Consumers' enthusiasm for the institution may change.

The Plan underscores E-ISAC's near-term objective to build and maintain membership and mentions useful areas for value-add. This is welcomed. E-ISAC's services and products could be better tailored to

resource-constrained stakeholders whose core businesses do not include selling power. For example, participation in the Cybersecurity Risk Information Sharing Program managed by E-ISAC has grown primarily for entities that pass the subscription costs onto consumers, whereas more cost-sensitive entities need to see a more robust net benefit proposition to justify participation. The effects of the new pilot project on participation should be incorporated into future cost structure considerations.

The value of E-ISAC sharing risk mitigation strategies and data and analysis depends on the suitability of its format and delivery parameters for the end user. Large Consumers already have detailed internal protocols to identify and mitigate operational cyber risk, and the nature and value of mitigating their information gaps varies. Large Consumers often factor in operational considerations for their facilities differently than utilities and thus their data needs differ. A stronger emphasis on contextualizing risk mitigation strategies and data analytics to non-utility stakeholders' needs would help enrich the value of E-ISAC services.

Contextualizing information better would help accomplish the Plan's objective to leverage threat information better to provide timely and actionable information. Routinized feedback from stakeholders will be important to strike the proper balance between information quality and expediency, as well as to inform E-ISAC on the types of information most useful to protect critical infrastructure (e.g., value-add to other subscription services that may come with vendor contracts). A particular area of value-add is to enable more expeditious transfer of classified information as the private sector often cannot procure these services in the marketplace.

E-ISAC's intent to improve collaboration with other strategic partners should emphasize other ISACs in industries that cover Large Consumers' registered entities. The Plan recognizes the need to do so with the MS-ISAC and DNG-ISAC, which is prudent given interstate commerce and natural gas-electric industries' interdependencies. It should also consider the ONG-ISAC and IT-ISAC.

Fulfillment of E-ISAC's mission could justify a rapidly ever-increasing budget, and thus cost-benefit tradeoffs should be recognized to permit proper budget scrutiny. At minimum, the development of valuations for E-ISAC's service would help inform prioritization of scarce resources. Large Consumers support the planned use of cost-benefit analysis for automated information sharing and would like to see the technique applied broadly across E-ISAC services.

Recommendations for other E-ISAC Areas

NERC should also work to alleviate concerns that inhibit E-ISAC membership recruitment, including those regarding the opacity of E-ISAC's strategic direction as it transitions to the Department of Homeland Security's multi-infrastructure framework. The current E-ISAC Code of Conduct lacks safeguards to protect against entities' information from being used in a purpose outside of the scope of E-ISAC's mission. In particular, entities that bear the costs of critical infrastructure protection (CIP) standards seek assurances that information submitted to E-ISAC will not result in cost-additive changes to CIP standards.

NERC established E-ISAC to catalyze *voluntary* information sharing within the electricity industry, but the Federal Energy Regulatory Commission (FERC) appears intent to use it as a conduit for setting *involuntary* reliability standards. As of January 2020, FERC and NERC do not appear to agree on the role of information collected under E-ISAC with respect to standards setting. FERC even went as far as to say that they "are concerned that NERC believes that the only information it can use from the E-ISAC to

inform Reliability Standards development is the information contained in the public reports" and requested a NERC filing to help FERC better understand how E-ISAC informs the development of Reliability Standards.[1] Last month, NERC submitted an answer that correctly articulated why NERC sought to establish a clear separation between E-ISAC and its mandatory compliance and enforcement functions in 2012.[2] Given FERC's posture, NERC and the E-ISAC's should endeavor to codify functional separation for E-ISAC as integral to achievement of its strategic objectives.

Relatedly, the E-ISAC would benefit from better characterization of its prospective activities relative to its mission. Some areas may be only tangentially related to its mission and be better addressed by another organization. E-ISAC should endeavor to avoid mission creep through mission alignment reviews of prospective areas and have safeguards against incessant incrementalism that can escape many standard measures of performance review.

[1] See Docket No. RR19-7-000, p. 67. https://www.ferc.gov/sites/default/files/2020-05/E-20_3.pdf
[2] See p. 14. https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14787441

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Lloyd A, Linke
Federal Utility/Federal PMA Portion Sector 4

DATE: August 4, 2020

SUBJECT: Response to Request for Policy Input to NERC Board of Trustees

The Portion of Sector 4 representing the Federal Utilities and Federal Power Marketing Administrations (Federal PMAs), appreciate the opportunity to respond to your July 15, 2020 letter to Ms. Jennifer Sterling, Chair NERC Member Representative Committee, requesting input on certain policy issues. The Federal PMA appreciates the opportunity to provide comments on the policy input on two matters of particular interest to the NERC Board of Trustees (Board) for their August 19-20, 2020 meeting.

- The Federal PMAs offers the following on Electricity Information Sharing and Analysis Center (E-ISAC) Long-Term Strategic Plan

  In summary the Federal PMAs is in support of the near term and long-term strategic plan outlined by E-ISAC. The Federal PMAs urge the Board to consider extending E-ISAC services and capabilities to support the communication sector, given cross-sector interdependencies members have on telecommunication platform for maintaining system reliability and system security during normal and emergency conditions. We would also like to see NERC and E-ISAC do more to encourage the industry to increase its capability to receive classified information.

- The Federal PMAs have no further input on Board request referencing amendments to the NERC Bylaws. We are is appreciative of NERC Staff in reviewing and proposing amendment for further clarifications of NERC bylaws.

The following are more specific responses to questions asked by the Board on the Policy Input Letter;

1. **Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?**

   The Federal PMAs believes the approach outlined by E-ISAC for near-term strategic plan and long-term strategic plan contains the appropriate elements. We appreciate the progress being made to-date and finds many of our key strategic elements have been factored in E-

ISAC plans. The Federal PMAs appreciate the E-ISAC long-term focus to "Enhance the E-ISAC's capability to better leverage classified and other critical threat and intelligence information (both nonpublic governmental and private sector) to provide timely and actionable information to the sector regarding security risks" However, we have concerns about the overall value to the industry if the industry doesn't expand the number of employees that have the appropriate security clearances to receive the information and suggest that the E-ISAC should include in their short-term focus regarding building and maintaining membership by demonstrating value through improved analysis, timely sharing of actionable information, collaboration with key government and strategic partners an effort to encourage the industry to increase their access to classified information.

2. **Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members??**

The Federal PMAs would like to see more work on telecommunication interdependency. E-ISAC long term strategic plan outlined "(4) extending E-ISAC services and capabilities to support the downstream natural gas sector, given cross-sector interdependencies." The Federal PMAs recommend that a similar assessment be done for telecommunication sector as many members, especially those in the WECC region, rely on telecommunication platform for system reliability and system security. The remedial action schemes are a major component of transmission infrastructure for the west due to long distance between generation resources and major load centers. Many of protective equipment are on communication platform to avoid system instability and facilitate cascading to prevent further damage to the BES.

The Federal PMAs appreciate the opportunity to provide this policy input to the NERC Board of Trustees.

ISO/RTO Council's (IRC) Policy Input to Board of Trustees

August 5, 2020

The ISO/RTO Council[1] (IRC) appreciates the opportunity to respond to the Board's request for policy input. The IRC offers the following input to the Member Representatives Committee (MRC) in response to Ms. Jennifer Sterling's letter dated July 15, 2020, regarding the Electricity Information Sharing and Analysis Center (E-ISAC) Strategic Plan and proposed amendments to the North American Electric Reliability Corporation (NERC) Bylaws.

Summary Comments

The IRC supports NERC's objective of better defining the E-ISAC's mission and priorities to focus resources on assisting the electric sector's protection against, and mitigation of the risks associated with, escalating cyber and physical security threats. The IRC is also supportive of the proposed NERC Bylaw Amendments presented at the July 22, 2020 MRC Informational Session. Our specific comments on the E-ISAC Strategic Plan are below.

1. Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?

We are generally supportive of the approach outlined in the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan. There are many other forums that currently provide information similar to what E-ISAC provides the Industry, such as Canadian governmental authorities and SysAdmin, Audit, Network and Security (SANS)[2]. We encourage NERC to review other available forums to identify duplicative efforts and streamline coordination to minimize the costs. The IRC encourages NERC to continue focus on E-ISAC identifying and sharing actionable information for Industry use in the most timely and cost-effective manner.

2. Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members?

Yes. We would encourage NERC to continue its efforts to optimize E-ISAC member value, which will require diligence in meeting the scope, and objectives put forth in the Strategic Plan. In the Policy Input Letter, NERC describes one aspect of E-ISAC's long-term focus as "extending E-ISAC services and capabilities to support downstream natural gas sector, given cross-sector dependencies." In the supporting materials, E-ISAC describes its long-term focus as "*evaluat[ing]* the benefits, costs, governance and funding issues, and options that extend E-ISAC services and capabilities to support the downstream natural gas sector…[3]". The IRC agrees

[1] The IRC is comprised of the Alberta Electric System Operator (AESO), the California Independent System Operator Corporation (California ISO), Electric Reliability Council of Texas, Inc. (ERCOT), the Independent Electricity System Operator of Ontario, Inc., (IESO), ISO New England, Inc. (ISO-NE), Midcontinent Independent System Operator, Inc., (MISO), New York Independent System Operator, Inc. (NYISO), PJM Interconnection, L.L.C. (PJM), and Southwest Power Pool, Inc. (SPP).

[2] Sans.org

[3] *See* Long-Term Update at p 3.

that E-ISAC should conduct analysis and evaluation before making a decision to "extend" E-ISAC's services and capabilities. The IRC suggests that it would make sense to focus first on understanding E-ISAC members' needs and experiences with regard to enhancing management of cyber and physical risks associated with the gas sector and then to leverage E-ISAC members to gather gas-related data input. For example, it would not be efficient for NERC to independently replicate data collection that is already occurring through E-ISAC members. In addition, the experience of our members suggests that there are jurisdictional issues that need to be overcome before NERC could directly access detailed gas pipeline and gas supplier operational data, including data on available inventories. Therefore, we ask NERC to be cautious expending resources on the Natural Gas Sector before these jurisdictional issues have been addressed, or if there is not clear value for the electric sector. We suggest limiting extension of the scope of E-ISAC services and capabilities until there is a clear understanding of the planned scope. In simple terms, it is better to start small and then expand the services and functionality once experience has been gained, rather than starting with a scope that is too ambitious.

Conclusion

The IRC appreciates the opportunity to provide policy input to the MRC for NERC's upcoming Board meeting.

Policy Input to the NERC Board of Trustees
August 20, 2020 Teleconference
Provided by the North American Generator Forum

The North American Generator Forum (NAGF) appreciates the opportunity to provide the following policy input in advance of the NERC BOT meeting.

Summary

Item 1: Electricity Information Sharing and Analysis Center (E-ISAC) Long-Term Strategic Plan

The NAGF appreciates the opportunity to provide policy input for the NERC Member Representatives Committee ("MRC") and Board of Trustees ("Board") in response to BOT Chair Roy Thilly's letter dated July 15, 2020. The NAGF agrees with and supports the updated E-ISAC draft Strategic Plan near-term and long-term strategic and operational focus.

Discussion

Item 1: Electricity Information Sharing and Analysis Center (E-ISAC) Long-Term Strategic Plan

The Board requests MRC policy input on the following:

1. Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?

The NAGF agrees with the primary focus of the updated E-ISAC near-term draft Strategic Plan to improve the effectiveness and efficiency of current products, platforms, and services. Maintaining focus on its core activities and continuing to produce products/services that helps to improve or inform stakeholder security posture and encourage stakeholder information sharing is critical to the protection of critical infrastructure.

The NAGF also agrees with the focus of the updated E-ISAC long-term draft Strategic Plan to provide additional value to members via greater

engagement with industry/government/private sector, improved information sharing, and enhanced analysis capabilities. This long-term vision supports the fundamental mission of the E-ISAC to reduce cyber and physical security risk through quality analysis and timely sharing of actionable electric industry security information.

2. Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members?

The NAGF has not identified any other areas or activities for consideration regarding the updated draft E-ISAC Strategic Plan.

NPCC, Inc.
NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

Policy Input
From a Northeastern North American Reliability Perspective
By the NPCC Board of Directors

1. **E-ISAC Near-Term Operational Focus Areas**
   - The NPCC Board supports the operational focus areas in the updated draft Strategic Plan, including enhancing the E-ISAC partnership and capabilities with Regional Entity situation awareness staffs, Canadian industry, law enforcement agencies and government entities.
   - To further its objectives, the NPCC Board recommends E-ISAC engage in active coordination with the numerous ongoing security initiatives within the ERO Enterprise to efficiently and effectively realize the complimentary goals of enhancing physical and cyber security through risk identification and mitigation.

2. **E-ISAC Long-Term and Additional Strategic Focus Areas**
   - In its long-term focus, the NPCC Board recommends that the E-ISAC expand opportunities and partnerships by establishing processes and procedures to capture Distributed Entergy Resources' (DER) related physical and cyber security information and by providing enhanced analysis capabilities, given the growth and inter-dependency of DER with the Bulk Power System and the Internet.
   - The NPCC Board supports expanding the E-ISAC's ability to interact and coordinate with Information Sharing and Analysis Centers from other related sectors (gas, telecommunication, etc.) to better address cross-sector reliability inter-dependences.

Affirmed by the NPCC Board of Directors
August 4, 2020
For submittal to the August 20, 2020
NERC MRC and BOT Meetings

Cooperative Sector Policy Input to the NERC Board of Trustees
August 5, 2020

The Cooperative Sector appreciates the opportunity to provide policy input to the NERC Board of Trustees (BOT) for policy issues that will be discussed at the August 19/20 NERC MRC, BOT and BOT Committee meetings.

Summary of Policy Input

- *The Cooperative Sector agrees with the primary focus of the E-ISAC Long-Term Strategic Plan Update and we have some concerns that we are requesting to be addressed:*
  - *Some near-term efforts may be more appropriately identified as longer-term efforts.*
  - *Metrics are needed to align more closely with both the near-term and the longer-term goals and objectives.*
  - *Support extending services to the downstream natural gas sector on a for-cost basis.*
  - *Encourage the E-ISAC to find ways to provide CRISP services at a lower cost for smaller entities.*
  - *Need more information about the proposed cyber security advisory group before announcing support and request the same information about the existing physical security advisory group.*
  - *Support enhancing the E-ISAC portal and we provide a few recommendations.*

Electricity Information Sharing and Analysis Center (E-ISAC) Long-Term Strategic Plan

- The Cooperative Sector appreciates the efforts of the E-ISAC to improve information sharing across the electricity subsector. Additionally, we appreciate the E-ISAC's collaborative approach to the development of its near-term and long-term plans engaging with industry, and through the Electricity Subsector Coordinating Council (ESCC) and the Member Executive Committee (MEC) in order to align its goals with the needs of the sector. After review of the E-ISAC Long-Term Strategic Plan Update, the Cooperative Sector agrees with the primary focus of the E-ISAC to improve the effectiveness and efficiency of current products, platforms, and services. We further agree that a near-term focus on core activities of the E-ISAC will provide substantial value in improving and informing the security posture of the electricity subsector.

- The Cooperative Sector is concerned that some of the near-term efforts may be ambitious and could more appropriately be identified as longer-term efforts. To ensure that efforts are appropriately resourced, that interdependencies are accommodated, and that longer-term efforts can leverage lessons learned and progress gained through near-term effort, we would encourage the E-ISAC to review its near-term and longer-term efforts to ensure that they are appropriately classified within the strategic plan's framework. For example, enhancements to information sharing through the portal and other bidirectional automated data sharing may be phased efforts that begin in the near-term, but do not reach completion within the near-term time frame.

- The Cooperative Sector supports the need to enhance the information sharing portal. In particular, efforts to make critical or timely information stand out from other general information sharing reports would be extremely valuable. As an example, the E-ISAC has effectively implemented a Critical Broadcast Program (CBP) for issuing All Points Bulletins (APBs) to industry. However, those APBs are not highlighted within the structure of the portal and there does not appear to be a way to subscribe separately to APBs. Accordingly, a welcome enhancement would be to add the ability to subscribe to APBs as well as functionality that highlights critical information such as the APBs. We also recommend that the portal enhancement-related goals take into account modifications and guidance necessary to facilitate the implementation of the upcoming reporting changes as a result of the implementation of

reliability standard CIP-008-6 and seek clarification that the proposed portal enhancements include such necessary changes. Finally, to ensure that users can effectively navigate and leverage the portal's functions and capabilities, the Cooperative Sector encourages the E-ISAC to consider increasing opportunities for simple on-demand user training of portal functions.

- The Cooperative Sector recommends that the E-ISAC add metrics to align more closely with **both** the near-term and the longer-term goals and objectives of the organization. As an example, the metrics proposed for analysis don't seem to hew closely to the goals and don't address timeliness, which is a key factor to threat containment. As well, the metrics proposed for information sharing do not appear to focus on the quality and usefulness of information, which is a key characteristic to demonstrating the value of information sharing to E-ISAC members. Finally, the goals identify objectives such as operationalizing existing agreements. These activities appear to have measurable characteristics, timelines, and activities. Accordingly, the E-ISAC should consider metrics associated with those goals.
- The Cooperative Sector supports extending services to the downstream natural gas sector on a for-cost basis. Such extension of services should reduce overall costs as the core E-ISAC infrastructure is already in place and any formal collaboration/information sharing/consistency can only benefit the security of critical infrastructure and is highly encouraged.
- The Cooperative Sector supports the E-ISAC's efforts to explore ways to further leverage Cybersecurity Risk Information Sharing Program (CRISP) and/or similar technologies to benefit smaller entities. Specifically, we encourage the E-ISAC to explore and determine the ability to provide CRISP services at a much lower cost for smaller entities.
- The Cooperative Sector is not opposed to a cyber security advisory group and, depending on the structure, scope, and membership, could support this proposal, but must, first, clearly understand important details such as how members will be selected and the extent they will be advising the E-ISAC on cyber security matters. Accordingly, the Cooperative Sector would request clarification and additional information on this proposal, and we have the same questions for the existing physical security advisory group.

Submitted on behalf of the Cooperative Sector by:
Barry Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association (NRECA)
703.907.5781
Barry.lawson@nreca.coop

NERC Board of Trustees
Teleconference
August 19-20, 2020
Policy Input of the Merchant Electricity Generator Sector

Sector 6, Merchant Electricity Generator Sector, takes this opportunity to provide policy input in advance of the upcoming North American Electric Reliability Corporation (NERC) Member Representatives Committee (MRC) and Board of Trustees (Board) meetings.

In a letter to MRC Chair Jennifer Sterling dated July 15, 2020, Board Chair Roy Thilly requested MRC input on the E-ISAC Long Term Strategic Plan through two questions. Sector 6 makes the following comments in response.

Key Point

- The Merchant Electricity Generators generally support the direction of the strategies and areas of focus for the E-ISAC Long Term Strategic Plan with no new suggestions or additions.

Sector 6 Comments for Policy Input

1. *Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?*

   The Merchant Electricity Generators agree with the updated draft of the E-ISAC Long Term Strategic Plan. The flexibility of implementing the elements within the strategic plan allows the E-ISAC to be nimble. The E-ISAC has proven to be effective and adaptable in the recent past and this strategic plan addresses the core issues for improving communication, analysis, and assistance while giving the E-ISAC the ability to adapt to changing needs.

2. *Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members?*

   The Merchant Electricity Generators are satisfied with the general direction of the near-term and long-term strategies and the areas of focus. We have no additional recommendations.

Sincerely,
/s/
Sector 6 Merchant Electricity Generator Representatives:

Martin Sidor
NRG Energy, Inc.

Sean Cavote
PSEG

MEMORANDUM

TO: Roy Thilly, Chair
NERC Board of Trustees

FROM: Carol Chinn
William J. Gallagher
Roy Jones
John Twitty

DATE: August 5, 2020

SUBJECT: Response to Request for Policy Input to NERC Board of Trustees

---

The Sector 2 and 5 members of the NERC Member Representatives Committee (MRC), representing State/Municipal and Transmission Dependent Utilities (SM-TDUs), appreciate the opportunity to respond to your July 15, 2020 letter to Jennifer Sterling, Chair of the MRC that requested MRC member sectors to provide input on NERC's Electricity Information Sharing and Analysis Center's (E-ISAC) strategic plan and budget. Specifically, the near-term and long-term strategic and operational focus areas described in the recent plan update. Additionally, the SM-TDUs appreciate working with NERC on the Bylaw revisions mentioned in the letter and we look forward to discussing the E-ISAC Strategic plan and the bylaw revisions during the virtual meetings of the Board of Trustees (Board), Board committees, and the MRC, on August 19-20, 2020.

Summary of Comments

- **E-ISAC Strategic Plan and Budget**
  - **SM-TDUs support the E-ISAC strategic plan and budget and the updated operational focus areas. The priority area for the E-ISAC should be improving the quality and timeliness of actionable information.**
- **NERC Bylaw Revisions**
  - **SM-TDUs appreciate NERC's outreach and willingness to work with stakeholders regarding Bylaw revisions.**

E-ISAC Strategic Plan and Budget

1. Do you agree on the near-term and long-term strategic and operational focus areas described in the updated draft of the Strategic Plan?

2. Are there any other areas on which you would recommend the E-ISAC focus its resources to fulfil its mission and bring additional value to its members?

The SM-TDUs strongly support the near-term and long-term strategic draft plan for the E-ISAC. The draft near-term plan to build and maintain membership through value provision is in line with the E-ISAC development of a solid foundation. Public power utilities especially appreciate the E-ISAC's efforts regarding member information sharing and increasing membership of public power utilities. The longer-term goal of improving the E-ISAC's capability to better utilize classified and other critical threat and intelligence information (both nonpublic governmental and private sector) to inform utilities so that they can act on emerging security risks is also supported by the SM-TDUs.

Keeping utilities informed about threats and providing actionable and easily understandable information is the key role that the E-ISAC plays for public power utilities. The E-ISAC needs to be a trusted partner with government intelligence resources that can take threat information and make it actionable to ensure that reliable power provision goes on uninterrupted. Consequently, the E-ISAC's continually improving relationship with the Department of Energy is encouraging. Providing utilities with higher valued information, should enable greater information sharing with and by utilities. Public power believes that the E-ISAC's information sharing priority in its strategic plan will get more utilities engaged in information sharing. Achieving the appropriate give and take of quality information will be critical to utility cyber security and mitigating physical and cyber threats. Utilities gaining greater quality threat information is especially critical regarding threats from foreign adversaries in the global threat environment.

SM-TDUs are encouraged by greater participation in the E-ISAC by public power utilities. The increase in over 10 percent of new public power E-ISAC members over the past year is a good indication that utilities will pursue greater information to bolster their security programs. Beyond E-ISAC membership there was also a significant increase in participation by public power utilities in the 2019 GridEx V exercise. These increases serve as proof that utilities value participation in E-ISAC security efforts as a "carrot" rather than a "stick." Smaller non-Bulk Electric System (BES) utilities are beginning to increase their participation in E-ISAC efforts to improve their security programs, rather than because of mandatory compliance.

Some SM-TDU utilities are members of E-ISAC and Multi-State Information Sharing and Analysis Center (MS-ISAC). Therefore SM-TDUs look forward to the future collaboration of the E-ISAC and MS-ISAC documented by the February 2019 Memorandum of Understanding (MOU) between the two organizations.

The E-ISAC current flat budget for 2020 and 2021 as the organization finishes out the initial 5 year plan is a significant achievement given that recently the E-ISAC has advanced to 24 (hour) by 7 (day) security operations. The SM-TDU's also appreciate and support the organizations move to using service providers to supplement operations and technology initiatives.

A specific item that public power advocates for 2021 E-ISAC budget funding would be that the E-ISAC be able to fund the development of an automated capability to participate in the integration of OT monitoring pilots for small to medium utilities. Such funding will allow the E-ISAC to accept data from small and medium utilities. This would facilitate greater security surveillance for smaller public power utilities' security programs going forward.

Going forward with its longer-term goals, the E-ISAC is in a unique position to provide security information to the energy industry, including smaller entities. Public power believes the plan to increase the value of E-ISAC offerings should continue to improve, the new CEO should be provided ability, resources and time to increase E-ISAC's value, and its staff has expertise that will help improve E-ISAC. Additionally, the E-ISAC should continue to look for ways to improve automated information sharing programs with SM-TDU's through collaboration IT and OT sensor programs.

Bylaws

SM-TDUs appreciated being able to work with NERC staff on the NERC bylaw revisions that the Board will consider a draft of during the August 2020 virtual meeting. It was important that during the COVID-19 time that there be sufficient stakeholder outreach. Such outreach provided the measured consideration that is needed for important rule changes.