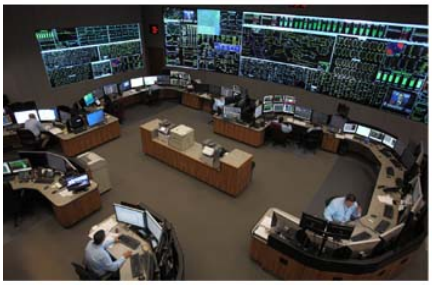
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Long-Term Strategic Plan Update

October 2020

RESILIENCY | RELIABILITY | SECURITY




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

TLP:WHITE

Executive Summary

October 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 develop, refine, and track metrics to measure progress.

In 2019, the E-ISAC took steps to improve the efficiency of operations and prioritize higher impact 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 focused on developing Portal postings and products that offer greater context and more actionable information. In addition, the E-ISAC 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, including work undertaken with partners, to ensure value to E-ISAC members
- Work closely with the Member Executive Committee working group, government, and industry partners to identify and share operational technology risks and risk mitigation strategies

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

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

TLP:WHITE

- 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
- Conduct a detailed evaluation of the pros, cons, costs, governance and funding issues, and alternatives to extending services and capabilities to support the downstream natural gas sector given cross-sector interdependencies

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. 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
October 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. Department of Energy (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 (ERO).

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

[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

alignment between priorities, optimize resource allocation, and establish metrics to measure progress.[6] The 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 across North America, 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. As the E-ISAC addresses its strategic plan, it will continue to

[6] The E-ISAC's annual departmental performance metrics are subject to review and feedback from both the Member Executive Committee and the NERC Board of Trustees. The NERC Board of Trustees, through its Corporate Governance and Human Resources Committee, also provides oversight of the E-ISAC's annual work plan priorities. NERC provides progress reports quarterly to the committee as part of the ERO Work Plan Priorities Update during the committee's quarterly open meeting. Both the E-ISAC department metrics and Work Plan priorities will continue to be refined and updated over time as the E-ISAC matures. The E-ISAC's 2020 performance metrics are included in Attachment 1. The E-ISAC's 2020 Work Plan Priorities may be found here under Focus Area 3: Build a Strong E-ISAC Based Security Capability.

TLP:WHITE

coordinate across the ERO Enterprise to ensure effectiveness and efficiency with respect to E-ISAC support for ERO Enterprise initiatives that enhance physical and cyber security through risk identification and mitigation.

The following is a summary of actions the E-ISAC will be undertaking to address these gaps and opportunities.

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 enhance the E-ISAC's reach to members and partners and avoiding or deferring those that disperse the E-ISAC's focus
- Exploring opportunities to refine and increase the effectiveness and efficiency of operations[7]

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 analysis, 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

[7] 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.

TLP:WHITE

national security.[8] It has never been more important for the E-ISAC to maintain its focus on its core activities and continue to develop products and services to provide stakeholders with content that helps improve or inform their security posture, encouraging them to share information in turn. The E-ISAC will continue to tailor products and services to meet the unique needs of the E-ISAC's diverse members, including those members that are resource constrained. Finally, the E-ISAC will continue to identify and review threats for its membership and, when possible, minimize duplication; at the same time, the E-ISAC recognizes that different jurisdictions may approach and respond to threats differently. 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.

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 delivering measurable value and 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 aims to increase industry participation and feedback regarding E-ISAC information-sharing programs, capabilities, products, and services. It will continue to coordinate with Canadian members to ensure products, platforms, and services meet the collective needs of the North American electricity industry and minimize unnecessary duplication where possible. The E-ISAC will also ensure Canadian participation in key activities, such as the MEC, the ESCC, and GridEx.

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.

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

TLP:WHITE

- **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. This feedback will serve as a critical input in the E-ISAC's ongoing efforts to improve the services it provides to its members.
- **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. These exploratory activities will take place in the near term, while evaluating success will be a longer-term effort.

Information Sharing[9]

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 nine 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, one large public provincial Canadian utility with over 5,000 employees, and one Reliability Coordinator.

Willingness to share information varies across the industry, and barriers include the time and effort required to share information.[10] 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,

[9] 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.

[10] 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

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 weekly or monthly basis and assists in performing trending analyses.
- **Phone Calls and E-mail 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. The E-ISAC is launching several initiatives in 2020 to achieve these focus areas; some will be completed in the short-term timeframe while others are ongoing initiatives.

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.

TLP:WHITE

In 2019, members shared significantly more physical security information than previous years.[11] 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, white papers, and services that bring value to the E-ISAC's members as well as ways to increase member physical security information sharing.

The E-ISAC will also explore, with members and other stakeholders, 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.[12] The E-ISAC will also work with the MEC working group and trade associations to continue to engage and educate members regarding the benefits of information sharing and drive further increases in information sharing.

Improving and Expanding Automated Information Sharing

The E-ISAC is exploring ways to enhance and expand automated information sharing and minimize duplication with other information sharing initiatives. As the E-ISAC considers different initiatives, these efforts will take a phased approach, beginning in the near-term, but may not reach completion within the near-term time frame. Steps the E-ISAC is taking to improve and expand automated information sharing 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

[11] 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.

[12] 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

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 new types of operational technology data 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 just one of several information sharing channels,[13] 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-ISAC's physical security team built new strategic relationships with the U.S. National Counterterrorism Center and the Royal Canadian Mounted Police, which culminated in both organizations providing briefings to members at GridSecCon 2019. The E-ISAC expects to deepen these relationships in the coming years, providing a valuable partnership and resource to enhance information sharing.

[13] 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

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 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 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, the Department of Homeland Security (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,[14] voluntary member shares, information from partners, and open-source information. E-ISAC

[14] 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

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 CRISP, 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 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.
- **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 (DNG-ISAC). The objectives of each of these agreements are 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. While evaluating progress over time is ultimately a long-term effort beyond 2021, in the short-term, the E-ISAC has developed evaluation criteria and is actively evaluating progress to establish a baseline with each collaboration agreement. Management will also explore similar collaboration initiatives with other strategic partners after assessing the potential benefits and supporting resource requirements. While the E-ISAC's priorities are primarily focused on the electricity industry, the partnerships with the MS-ISAC and the DNG-ISAC—and discussions with other cross-sector organizations, like the Financial Sector ISAC and the Communications ISAC—will provide greater insight into threat identification activities, potential impacts, and mitigation strategies across sectors. As the E-ISAC develops these and other partnerships, it will do so with the understanding of member needs and communicate these partnership objectives to E-ISAC members. Through these partnerships, the E-ISAC will continue to focus on providing timely and actionable information to its members and will

TLP:WHITE

communicate shared risks and interdependencies among sectors.

- **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. In addition to exploring ways to make CRISP more cost-efficient for lower-resourced organizations, 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 with 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 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. Both pilots included industry input to develop pilot requirements.

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 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 DHS 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.

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

TLP:WHITE

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
- Leveraging ERO Enterprise, electricity industry, inter-dependent critical infrastructures, and distributed energy resource expertise to identify emerging threat and risk vectors to the bulk power system, and develop enhanced cyber and physical security analytic capabilities to support industry in their efforts to mitigate these risks and enhance resilience
- 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, taking into account industry and other stakeholder input, of the pros, cons, costs, governance and funding issues, and alternatives to 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. Finally, we will also leverage capabilities already available from other agencies or partners, and optimize and further develop existing partnerships.

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
	A monthly webinar hosted by the E-ISAC featuring cyber and physical security updates as well as news	All AOO members

TLP:WHITE

Services (Workshops, Webinars, Working Groups, Platforms, Conferences, and Exercises)	Description	Audience
Monthly Briefing Series (Webinar)	and trends from partners, including government and cross-sector partners; recordings are posted to the Portal and content is incorporated into the Monthly Report	
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 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, products, and services and to share best practices and lessons learned with industry colleagues	Open to industry members, with a focus on analysts or those with information sharing responsibilities

TLP:WHITE

Services (Workshops, Webinars, Working Groups, Platforms, Conferences, and Exercises)	Description	Audience
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
Vulnerability of Integrated Security Analysis (VISA) Implementation Workshop	Designed to teach participants how to use the VISA 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