

Agenda

Technology and Security Committee

May 13, 2020 | 12:30-1:30 p.m. Eastern
Conference Call

Click to Join [Webinar](#)

Introduction and Chair's Remarks

NERC Antitrust Compliance Guidelines*

Agenda Items

1. **Minutes*— Approve**
 - a. February 5, 2020 Meeting
2. **E-ISAC Update*— Review**
 - a. COVID-19
 - b. Long-Term Strategic Plan Update
 - c. Preliminary 2021 Budget
3. **ERO Enterprise Business Technology Projects Update*— Review**
4. **ERO Enterprise Align Project *— Update**
5. **Establishment of the ERO Enterprise Secure Evidence Locker* — Review and Recommend to Finance and Audit Committee**
6. **Other Business**
7. **Adjournment**

*Background materials included.

Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

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

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

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

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

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

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

DRAFT Minutes

Technology and Security Committee Meeting

February 5, 2020 | 11:00 a.m. – 12:00 p.m. Pacific

Westdrift Manhattan Beach, Autograph Collection
1400 Park View Avenue
Manhattan Beach, California 90266

Chair Suzanne Keenan called to order a duly noticed open meeting of the Technology and Security Committee (the “Committee”) of the Board of Trustees (“Board”) of the North American Electric Reliability Corporation (“NERC” or the “Company”) on February 5, 2020, at 11:00 a.m. Pacific, and a quorum was declared present. The agenda is attached as **Exhibit A**.

Present at the meeting were:

Committee Members

Suzanne Keenan, Chair
Janice B. Case
Kenneth W. DeFontes
George S. Hawkins
Roy Thilly, *ex officio*

Board Members

Robert G. Clarke
Frederick W. Gorbet
Robin E. Manning
James B. Robb, NERC President and Chief Executive Officer
Jan Schori
Colleen Sidford

NERC Staff

Tina Buzzard, Associate Director
Manny Cancel, Senior Vice President and Chief Executive Officer of the E-ISAC
Shamai Elstein, Assistant General Counsel
Howard Gugel, Vice President, Engineering and Standards
Stan Hoptroff, Vice President, Business Technology
Ed Kichline, Senior Counsel and Director of Enforcement Oversight
Mark Lauby, Senior Vice President and Chief Engineer
Bill Lawrence, Vice President, ERO Enterprise Security Initiatives
Sônia Mendonça, Senior Vice President, General Counsel, and Corporate Secretary
Janet Sena, Senior Vice President, External Affairs
Andy Sharp, Vice President, and Interim Chief Financial Officer
Mechelle Thomas, Vice President, Compliance

Chair’s Remarks

Ms. Keenan welcomed the Committee members and highlighted recent Committee activities. She noted that on November 6, 2019, the Committee hosted the NERC Board of Trustees in a closed meeting to discuss NERC security issues, and will continue that briefing annually. Mr. Robb introduced

Mr. Cancel and Mr. Lawrence in their new roles as Senior Vice President and Chief Executive Officer of the E-ISAC and Vice President, ERO Enterprise Security Initiatives, respectively.

NERC Antitrust Compliance Guidelines

Ms. Keenan directed the participants' attention to the NERC Antitrust Compliance Guidelines included in the agenda, and indicated that all questions regarding antitrust compliance or related matters should be directed to Ms. Mendonça.

Minutes

Upon motion duly made and seconded, the Committee approved the minutes of the November 1, 2019 meeting as presented at the meeting.

E-ISAC Update

Mr. Cancel provided an overview of the Q1 2020 Member Executive Committee ("MEC") conference call held on January 23, 2020, referencing the materials provided in the advance agenda package. He highlighted the topics discussed on the MEC conference call, including: (1) the strategic plan update; (2) an update on 2020 performance metrics results; (3) member information sharing initiatives; (4) operations; and (5) strategic partner engagements. The Committee discussed additional opportunities to engage with Canadian entities and government partners, and the importance of creating an environment where registered entities feel safe sharing information with E-ISAC without compliance ramifications.

ERO Enterprise Information Technology Strategy and IT Projects Update

Mr. Hoptroff provided an update on the ERO Enterprise information technology projects, referencing the materials included in the advance agenda package. He provided an update on: (1) the status of the Align Project; (2) the status of the November release of the Centralized Organization Registration ERO System ("CORES") entity registration system enhancement; (3) the status of version 3 of the Situation Awareness for FERC, NERC, and the Regional Entities ("SAFNRv3"); (4) the development of additional analytical capabilities for the E-ISAC; and (5) the E-ISAC new customer relationship management system. The Committee discussed the timing for Align's release and the rollout schedule for evidence lockers.

ERO Enterprise Security

Mr. Lawrence presented on ERO Enterprise security initiatives. He shared best practices regarding security training, enhancing the ERO Enterprise response to grid emergencies, and protecting ERO Enterprise systems and data.

Annual Review of Committee Mandate

Ms. Mendonça noted that the Committee is required to review its mandate on an annual basis. She stated that the NERC Legal Department did not recommend any revisions to the Committee Mandate.

Adjournment

There being no further business, and upon motion duly made and seconded, the meeting was adjourned.

Submitted by,

A handwritten signature in black ink, appearing to read 'Sônia', is placed over a light gray rectangular background.

Sônia Mendonça
Corporate Secretary

Long-Term Strategic Plan

Action

Review

Background

The objective of this agenda item is to provide the Technology and Security Committee (Committee) with a brief update regarding the E-ISAC's progress to date, as well as present proposed updates to the E-ISAC Long-Term Strategic Plan.

As discussed at the Committee's February 2020 meeting, management is taking the opportunity to assess the Long-Term Strategic plan to:

- Confirm strategic and operational focus;
- Evaluate and refine products and services;
- Optimize resource allocation; and
- Identify additional areas to provide value to members.

Included in the read-ahead material is a revised draft of the Long-Term Strategic Plan. The E-ISAC's main focus areas are: (1) providing timely and actionable information to members; (2) enhancing its analysis of security threats and mitigation strategies; (3) improving collaboration with industry, U.S. and Canadian government partners, and other stakeholders; and (4) ensuring improvement and alignment across our three strategic pillars: engagement, information sharing, and analysis.

In the near-term (1-2 years), the E-ISAC will continue to focus on improving the effectiveness and efficiency of current products, platforms, and services. The E-ISAC will also sharpen its 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.

In the long-term (3-5 years), the E-ISAC will focus on providing additional value to members and other stakeholders in three key areas: (1) enhancing intelligence and analytic capabilities with an increased focus on operational technology risks; (2) developing enhanced capabilities to improve sharing of classified and other critical threat and intelligence information provided by government and other strategic partners; and (3) extending E-ISAC services and capabilities to support the downstream natural gas sector, given cross-sector interdependencies.

TLP:WHITE

Executive Summary

E-ISAC Strategic Plan Update

April 2020

Background

In 2017 the Electricity Information Sharing and Analysis Center (E-ISAC), with guidance from the Member Executive Committee (MEC), the North American Electric Reliability Corporation (NERC) Board of Trustees (Board), and various trade associations and stakeholder groups, developed a strategic plan (Strategic Plan) to better define its mission and focus its resources in helping the electric sector protect itself 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 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 also recognizes the critical interdependencies between the E-ISAC, industry, U.S. and Canadian government agencies, and other stakeholders.

During 2019, the E-ISAC took steps to improve the efficiency of operations and reduce or eliminate certain lower value activities. Leadership was strengthened and security operations reorganized to align and optimize cyber and physical security teams as part of an integrated watch operations team. Portal posting and other publications were also reorganized and enhanced to provide greater context and more information that is actionable. In addition, a performance management group was created 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 A summary of 2019 accomplishments includes:

- Establishing 24x5 watch operations and hiring experienced security operations staff to facilitate a migration to a 24x7 model by Q3 2020
- Launching a critical broadcast program to quickly disseminate information regarding imminent threats and other important notifications
- Increasing both inbound and outbound information sharing with members and government partners
- Supporting numerous U.S. Department of Energy (DOE) initiatives including Cybersecurity Risk and Information Sharing Program (CRISP) expansion and CATT 2.0
- Implementing a customer relationship management (CRM) platform based on the Salesforce platform
- Increasing and diversifying membership, both within the United States and Canada
- Establishing an Industry Engagement Program and increasing and diversifying participation in security exercises and training

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

TLP:WHITE

- Developing, in coordination with the industry supported Physical Security Advisory Group, a 2-year action plan to expand physical security risk identification, risk mitigation and preparedness
- Entering into detailed collaboration agreements with the Canadian Independent System Operator (IESO), the Downstream Natural Gas ISAC (DNG-ISAC) and the Multi-State ISAC (MS-ISAC)
- Building analytical capabilities and strengthening the E-ISAC's talent pool, including both cyber and physical security expertise.

As part of management's planning efforts for 2020 and 2021 and taking into account feedback from the Board, MEC, members and other stakeholders, it assessed progress to date, re-confirmed operating and strategic priorities, and identified both gaps and opportunities to further improve products, services and, ultimately, provide greater value to members. 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 services². 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, collaboration with key government and strategic partners, while ensuring that E-ISAC operations are both effective and efficient.

Key efforts will include:

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

Within these efforts in mind, we 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 Investments

- 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 our scope and avoiding or deferring those that disperse our focus
- Exploring opportunities to refine and increase the effectiveness and efficiency of our resource utilization supporting security exercises (e.g. GridEx), conferences (e.g. GridSecCon), and other

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

TLP:WHITE

resource intensive activities

Engagement

- Expand and diversify membership by leveraging industry data and our CRM platform to identify and target prospects and proactively engage with underrepresented segments of the industry including those in the public power segment
- Develop more robust mechanisms to obtain and act upon stakeholder feedback, and improve services for existing members

Information Sharing

- Increase the span, quality, and volume of voluntary shares from members
- Improve and expand automated information sharing in order to increase the timeliness and volume of sharing and reduce the effort required by members to share information with us and use information from us
- Work with our government partners to increase E-ISAC and industry access to classified information through threat briefings and collaboration
- Mature security operations processes to provide members with more timely and relevant information, leveraging our 24 x 7 security operations staffing

Analysis

- Improve the frequency, timeliness and quality of valuable, in-depth analysis and reports
- Operationalize the objectives described in agreements with DOE, IESO, DNG-ISAC and MS-ISAC
- Facilitate collaboration between U.S. and Canadian government agencies in support mutual priorities and programs including Pathfinder, Cyber Space Solarium³, Project Lighthouse and the recommendations of the National Infrastructure Advisory Council (NIAC)⁴
- Expand CRISP program participation, streamline governance, drive greater program value through data enrichment and analysis

Longer Term Focus (3-5 years)

For the long-term horizon (3-5 years), the E-ISAC will focus on providing additional value to members and other stakeholders in three key areas

- (1) enhancing intelligence and analytic capabilities with an increased focus on operational technology risks
- (2) developing enhanced capabilities to better share classified and other critical threat and intelligence information provided by government and other strategic partners
- (3) extending E-ISAC services and capabilities to support the downstream natural gas sector, given cross-sector interdependencies.

³ Cyberspace Solarium Report, March 2020

⁴ NIAC, Transforming the U.S. Cyber Threat Partnership Final Report, December 2019

TLP:WHITE

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.

DRAFT

TLP:WHITE

E-ISAC Long-Term Strategic Plan Update

April 2020

Background

The Information Sharing and Analysis Center (ISAC) construct was authorized by an U.S. presidential directive issued in 1998 and is focused on engagement, information sharing, and analysis directly related to the protection of critical infrastructure. The Electricity Information Sharing and Analysis Center (E-ISAC) was formed in 1999 in response to a request by the U.S. Secretary of Energy that the North American Electric Reliability Corporation (NERC) serve as the ISAC for the electricity sector.⁵ The E-ISAC's fundamental purpose and mission is to support its members and other stakeholders in reducing cyber and physical security risk through quality analysis and timely sharing of actionable electricity industry security information.

The E-ISAC is organized and operates as a separate department within NERC. Its operations and budget are primarily funded through NERC annual assessments paid by electric load serving entities in North America. Separate contractual funding is also provided by participants in the Cybersecurity Risk Information Sharing Program (CRISP) to support that program. CRISP was developed by the U.S. Department of Energy (DOE) and is managed by the E-ISAC.⁶

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)⁷ 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 a CEO-level executive, security executive, or subject matter expert 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 (BOTTSC), provides corporate oversight of the E-ISAC, giving due consideration to MEC recommendations. This governance helps ensure that the E-ISAC remains focused on the 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 (Strategic Plan) to better define its mission and focus its resources towards helping to protect the electric sector from escalating cyber and physical security risks. The Strategic Plan has three primary areas of focus - *Engagement, Information*

⁵ NERC was designated by the Federal Energy Regulatory Commission as the ERO under Section 215 of the Federal Power Act.

⁶ Fees from security conferences and training events also provide additional, less significant sources of funding.

⁷ 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

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 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:

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 electric sector 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 its planning efforts for 2020 and 2021 and taking into account feedback from the Board, MEC, members, and other stakeholders, management assessed progress to date, re-confirmed operating and strategic priorities, and identified both gaps and opportunities to further improve products, services, and,

TLP:WHITE

ultimately, provide greater value to members. 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:

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

Within these efforts in mind, we 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 our scope and avoiding or deferring those that disperse our focus
- Exploring opportunities to refine and increase the effectiveness and efficiency of operations⁸.

Building Trust and Improving Effectiveness of Current Products and Services

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 analytical, engagement, and management resources, and supporting systems to advance the objectives in the Strategic Plan. The recent 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.⁹ It has never been more important for the E-ISAC to maintain its focus on its core activities and continue to enhance its existing products and services. 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.

⁸ 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.

⁹ NIAC, Transforming the U.S. Cyber Threat Partnership Final Report, December 2019

TLP:WHITE

The E-ISAC's primary focus over the next two years will be on building industry and government engagement and trust, and refining and improving the effectiveness of existing products, services, and supporting platforms.

Engagement

Successful implementation of the Strategic Plan is dependent on ensuring that members and stakeholders are informed, involved, and have opportunities to interact and provide input. Above all, they must trust the organization and see value the products and services it provides.

The E-ISAC's core engagement efforts will be focused on building this trust and encouraging the collaborative exchange of information, ideas, best practices, and insights related to understanding, remediating, and mitigating security risks. Engagement efforts are also focused on increasing industry participation and feedback regarding our information sharing programs, capabilities, products, and services.

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

- **Expanding and Diversifying Membership** – Expanding and diversifying E-ISAC 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** – Enhancing stakeholder onboarding processes and engagements through the development of a more mature onboarding process.
- **Leveraging Our Customer Relationship Management Platform** – Fully implementing and maximizing use of our new Salesforce CRM platform to 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** – Exploring 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 evaluate partnering opportunities.

TLP:WHITE

Information Sharing¹⁰

Voluntary sharing of security threat, vulnerability, and event/incident information by members is critical to the achievement of the goals set forth in the Strategic Plan. Trusted, timely, sharing of information by E-ISAC members enables rich and highly contextual understanding of and mitigation of security risks.

While progress has been made in increasing information sharing by members, considerable work remains, including reducing real and perceived barriers to information sharing. As of the end of 2019, the E-ISAC has 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.¹¹ 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. The bulk reporting method, which is used currently by only a handful of members for physical security incidents, provides some efficiency but is typically done on a monthly basis and therefore is not as timely, although it assists in performing trending analyses. The Portal reports can be done on a timely basis, but 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 again in the E-ISAC system. Finally, phone calls and e-mails 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 (1) enhancing the information sharing portal to make it easier for members to share, manage, and find information, (2) increasing the span, quality, and volume of voluntary shares from members, (3) improving and expanding automated information sharing, and (4) improving the security watch operations availability and capabilities.

¹⁰ 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.

¹¹ 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 E-ISAC Portal:

- Driven by the 2019 MEC working group guidance:
 - Expand available structured information fields driven by sub-type events and incidents for both physical and cyber voluntary share postings
 - Redesign information-sharing account groups into more granular and discernable options
- Driven by efficiency, internal control needs, and leading ISAC best-practices, 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.
- Enhanced 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.¹² 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 is defined as sharing information about many incidents all at once, in a method that reduces the sharing burden on individual members. This voluntary process is tailored to the needs of individual members and can include sharing monthly summaries of incidents, transmission of security logs, or any other sharing method (i.e., 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. Our 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 our members, as well as ways to increase member physical security information sharing.

¹² 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.¹³ The E-ISAC will also work with the MEC working group and trade associations to continue to actively 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:

- Implementation of an automated information sharing pilot program in 2020 for a limited set of willing and capable members for voluntary sharing of information in a bi-directional fashion between external parties' applications and E-ISAC applications. The pilot will explore the feasibility of creating bi-directional 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 on-going 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, but only after sufficient due diligence is performed on the pragmatism of such an endeavor and if the lack of a sufficient alternative option(s) exists.
- 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 24/5 Watch Operations and will be moving to 24/7 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

¹³ 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,¹⁴ it plays an important role in building member trust and understanding of 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:

- 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 is also strengthening its working relationship with the Royal Canadian Mounted Police (RMCP). The team is co-authoring a white paper on Wind Farm security risks, exploring analyst exchange opportunities and is conducting RMCP 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. Ongoing collaboration with these entities is expected over the planning period.

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

- 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

During 2020, Management will be working closely with the DOE to operationalize this memorandum of understanding, including defining deliverables and schedules. The E-ISAC will also work closely with 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 support Pathfinder initiatives within the sector.

While E-ISAC has established some collaboration with federal partners at the classified level, it is important that the E-ISAC 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

¹⁴ 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

increasing need for public/private partnerships and information sharing in classified as well as unclassified venues. In addition to supporting NIAC, Cyber Solarium and Pathfinder initiatives, near-term and related E-ISAC activities involving classified arenas include working to:

- Improve E-ISAC access to classified information and threat briefings to further develop and steer programs such as CRISP and our threat information sharing to the sector
- increase meaningful classified threat briefings to the sector
- strengthen classified collaboration with DOE, DHS, and the National Security Administration
- Provide electricity fundamentals training to government partners in both classified and unclassified settings to both educate and provide awareness of the electricity sector 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: (1) information provided by CRISP participants,¹⁵ (2) voluntary member shares (3) information from partners; and (4) 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, unclassified briefings and reports are provided to participating members and anonymized information is shared with members through the E-ISAC portal, as well as with trusted partners subject to the terms of confidentiality agreements. On a less frequent, but often more critical basis, 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 four areas:

- **Increasing the Frequency of Valuable, In-depth Analysis** – Improving business processes and deploying technology to drive greater efficiency, freeing up resources to support the development and sharing of more valuable analytical products. Additional quantitative data analysis techniques will be leveraged for identifying observed security patterns and trends across the industry.
- **Improving the Quality and Timeliness of Reports** – Renewed focus on quality, relevancy and timeliness of information sharing in general, which will apply to reporting (the right reporting on the right subjects with the right quality at the right times). Progress will be driven through focus on the design and execution of supporting quality control processes, such as inbound and outbound product quality assessments.
- **Operationalizing Agreements with the IESO, MS-ISAC, and DNG-ISAC** – The E-ISAC recently entered into collaboration agreements with IESO, MS-ISAC, and DNG-ISAC. The objectives of each of these agreements is to strengthen information sharing with the goal of further enhancing analytical

¹⁵ Information provided by CRISP participants is analyzed by the Pacific Northwest National Laboratory within the strict confines of the CRISP program structure where it is subject to detailed data handling and other contractual protections. 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

products that can be shared with each of these organizations, their members, and other trusted stakeholders. Management has developed detailed work plans, with quarterly deliverables and schedules through 2020 and 2021, to further advance the underlying objectives of each of these collaborations. Management will also explore similar collaboration initiatives with other strategic partners after making an assessment of the potential benefits and supporting resource requirements.

- **CRISP: Expanding Participation, Driving CRISP Data Enrichment and Analysis –**

Participation in CRISP has grown significantly. DOE has also continued 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 planned to be initiated in 2020. The objective of this pilot is to explore ability to view and analyze security risks associated with both utility information system and operating system technologies and advance participant and stakeholder understanding of the threat landscape facing the utility industry.

In addition, while all registered users of the E-ISAC portal have access to postings of unclassified information derived from CRISP, given the current cost and complexity of the program, there are practical, financial and administrative limitations on the ability of smaller utilities to participate directly. 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.

A number of 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 further leverage this sensor information with other E-ISAC data sources, including CRISP, to allow the MS-ISAC to further enhance the services provided to these smaller government owned utilities.

The success of our 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 be focused on assessing the viability of looking across information and operating technology data to better identify the most critical risks and exploits targeting 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 our 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. In addition, as mentioned, an automated information sharing pilot is scheduled for 2020 and is aimed at reducing one of

TLP:WHITE

the information sharing barriers (cost and time to share) by eliminating redundant data entry and reducing data latency for those that chose to participate. The E-ISAC will also leverage enhanced case management and workflow to increase the effectiveness of timely and quality production of information products for our members. Finally, E-ISAC will use its CRM system to better track, target, and provide more meaningful and consistent interaction and messaging with our partners and members.

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

As we look at the longer term time horizon, the E-ISAC is considering several initiatives to provide additional value to our members and other stakeholders including:

- (1) enhancing intelligence and analytic capabilities with an increased focus on operational technology risks
- (2) developing enhanced capabilities to better share classified and other critical threat and intelligence information provided by government and other strategic partners
- (3) extending E-ISAC services and capabilities to the downstream natural gas sector, given cross-sector interdependencies.

In addition, the E-ISAC will evaluate additional partnership opportunities with the commercial sector, other ISACs, and government sponsored research and development organizations. The E-ISAC will work closely with stakeholders and government partners to carefully evaluate the benefits and potential challenges of each of these initiatives, as well as in the formulation of appropriate program activities, budgets and schedules.

TLP:WHITE

Attachment 1

2020 Performance Metrics		
Engagement		
% increase in prospective member organizations engaged	% increase in diversity of types of member organizations participating in Industry Engagement Program and E-ISAC led workshops	% increase in cross-sector participation in GridEx
% increase in prospective member organizations that sign up to use the E-ISAC portal.	% increase in Canadian member organizations	% 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)	% increase in GridEx participation	
Analysis		
% increase of content enriched by E-ISAC analysts	% 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: % 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: % increase in number of information shares by source, channel, and event type	Member Information Sharing: % increase in quality and unique value-add information received from member organizations	Security Watch Operations coverage: <ul style="list-style-type: none"> • On Duty – Core Hours Head Count • On Call – Off Hours Head Count • On Duty – Off Hours Head Count
Partner Information Sharing: % increase in volume of information shares received from partner organizations % increase in quality of information shares received from partner organizations	% increase in targeted feedback from members and partners	Security Watch Operations sharing: IOCs 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 which includes monthly trends and analysis that industry members can use to help inform products for industry leadership.	All 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
Government Reports	Posting of government reports with additional E-ISAC analysis as needed. Provides situational awareness of reporting from government entities.	AOO cyber and physical analysts
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 bi-directional sharing of information between E-ISAC members, partners, and staff.	All members and partners with Portal access
CAISS (IOC feeds)	Provides participating members with a daily, automated feed of indicators of compromise based on the STIX/TAXII protocol.	Participating AOO members

TLP:WHITE

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
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 co-hosted by NERC, the E-ISAC, and a rotation of NERC Regions. 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 electric companies. CRISP is a private-public collaboration coordinated by the E-ISAC between the U.S. Department of Energy (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. Includes a classified briefing for cleared participants.	CRISP members
Industry Engagement Program	A 3-day program for small groups of industry analysts to gather at the E-ISAC DC 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

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 DBT methodology to enhance the physical security of assets.	AOO security personnel and analysts
Securing the Grid (Classified Workshop)	The E-ISAC partners with the MITRE Corporation to plan and host the Securing the Grid classified workshop. The event included industry AOs to identify resilience gaps and opportunities. Invited participants from government and industry offer solutions and ideas to address various industry challenges.	AOO senior management and CEOs
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 (SEWG), weekly government-industry call, and the Member Executive Committee (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 Bulk Electric System 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

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

E-ISAC Strategic Plan

Manny Cancel

Technology and Security Committee Open Meeting

May 13, 2020

RELIABILITY | RESILIENCE | SECURITY



- COVID-19
- Landscape Assessment
- Progress to Date
- E-ISAC Strategic Plan
- Resource Focus
- Near-Term Focus
- Long-Term Focus
- Keys to Success

E-ISAC has been actively tracking COVID-19 since February 2020

- Business continuity plan activated and entire E-ISAC working remotely
 - Watch Operations fully staffed
 - CRISP online and functioning
- Portal postings and Level 2 NERC Alert issued
- Engaging and supporting Government partners
- Participating in ESCC Tactical Tiger Teams
- Maintaining contact with Tri-Sector entities

- Quantitative assessment of critical infrastructure ISACs conducted
- Key Findings:
 - The E-ISAC is a well-established organization, with comparable resources and offerings to the top tier of the assessment group (the Financial Sector and Multi-State ISACs)
 - The E-ISAC is financially sound, with appropriate costs relative to staffing and offered products and services
 - Opportunities for improvement include project prioritization, demonstrating the value of and increasing member information sharing, and increasing membership of public power

Organizational Changes:

- Leadership and other key positions strengthened
- Security operations reorganized and 24x7 Watch established in shakedown mode
- Performance Management Group established and formal project management principles adopted

Operational and Other Improvements:

- Increased information sharing and Critical Broadcast Program
- Cybersecurity Risk Information Sharing Program (CRISP) governance improved; CRISP expansion continues
- Customer relationship management system implemented and membership expanded
- Memorandums of Understanding (MOUs) executed with Independent Electricity System Operator, Department of Energy, and other ISACs
- Performance metrics put in place (See Appendix)

24x7 Staffing in Place (Remote)

- Fully Operational in Q3 2020 or sooner
- Cyber and Physical security watch shifts in place staffed by employees and contractors
- Two week schedules in place and adjusted as needed
- Key Functions
 - Threat Analysis
 - Portal Postings and Administration
 - Process Improvement
 - Training, Drills, and Procedure Development

Cyber

- **COVID-19 Threats**
 - HHS Denial of Service (DoS) attack
 - Remote access and collaboration facilities
 - Disinformation, spearphishing, and credential harvesting
- **U.S. / Iran Tensions**
 - Activity is reduced but Iranian threat actors remain active
- **Other Threats**
 - ICS Supply Chain
 - Collaboration sites (DropBox, Google Drive, O365)
 - Phishing and credential harvesting
 - Ransomware and destructive wiper malware

Physical

- **Theft**

- Represents 47% of the total incidents shared with the E-ISAC
- Copper theft accounts for 50% of thefts
- Most incidents (42%) are in substations

- **Intrusions**

- Trespassing and intrusion account for 21% of incidents
- Most incidents (51%) are in substations

- **Surveillance**

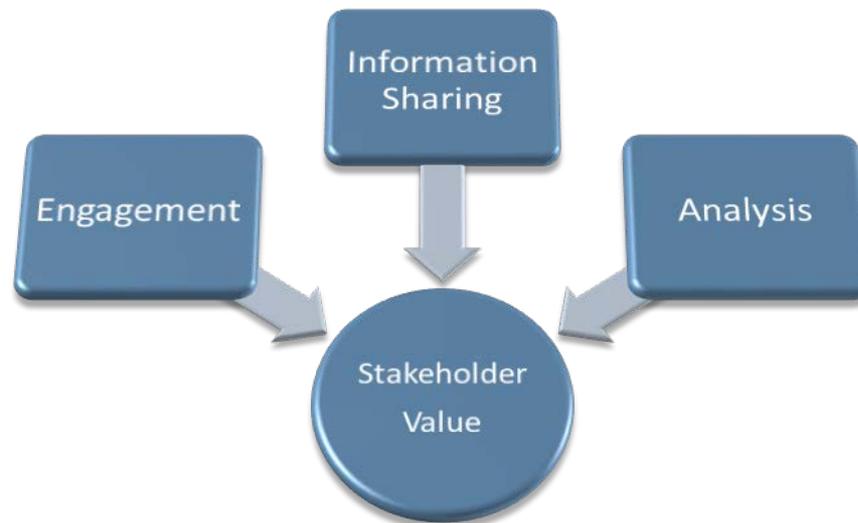
- Suspicious photography, reconnaissance and drones account for 11% of incidents shared

- New governance framework in place
- Operational Technology (OT) Pilot in progress
 - RFP sent to vendors, final responses due May 15
- System Log Pilot
 - Assimilate logs into CRISP and enhance ability to check for threats
 - Target for production Q1 2021
 - Will be incorporated into 2021 CRISP budget
- Medium and Small utility cooperative initiative
 - In discussions with DOE, NRECA, and APPA

- Events
 - Schedule under review and upcoming events switched to web conferences
 - March IEP and GridSecCon canceled due to coronavirus/travel restrictions
- Member Feedback Strategy
 - Formalize process to collect, manage, and respond to member feedback in Q2 2020
 - Create and implement member feedback survey (bi-annual)
- Designated Approving Official Rollout
 - Enhance member onboarding experience
 - Streamline internal processes for onboarding/vetting
 - Members knowledge and control of Portal access by their organization
 - Improved ability to communicate with member organizations

Focus Areas:

- Timely and actionable information
- Analysis regarding security threats and mitigation strategies
- Improved collaboration with industry, U.S. and Canadian government partners, and other stakeholders
- Continuous improvement and alignment across our three strategic pillars



- Maximize resource utilization
- No significant personnel increases
- Evaluate and prioritize strategic relationships
- Effectively increasing information sharing
- Assess ability to add significant value to members through internal data enrichment strategies and investments
- Define role regarding operational technology risk identification, assessment, and information sharing

Organizational Initiatives

- Continue to foster an inclusive work environment, optimize organizational structure
- Refine succession plan for key roles
- Establish 24x7 Security Operations
- Consider use of service providers to supplement operations, technology initiatives, and key conferences (GridSecCon and GridEx)

Operational and Other Improvements

- Demonstrate the value of increased information sharing
- Support U.S. and Canadian government initiatives
- Complete CRISP +30 and Operational Technology (OT) pilot and evaluate other sensors
- Use feedback to improve member services and increase membership in underrepresented areas
- Operationalize and extract value from recently executed MOUs

- High Priority Partnership

- Formalize and expand engagement and collaboration
- Explore data sharing opportunities



- Other Partnerships and Relationships

- Nurture with reduced E-ISAC resource commitment



- Adopt a broader focus on OT risks
- Develop enhanced threat and intelligence analytics
- Extend services to the downstream natural gas sector
- Continue to evaluate partnership opportunities with:
 - Commercial sector
 - Other ISACs
 - Government sponsored research and development organizations

The E-ISAC will engage stakeholders and government partners to carefully evaluate the benefits and potential challenges of each of these initiatives

- Allocating resources more effectively
- Demonstrating the value of information sharing
- Improving decision-making and governance
- Enhancing project prioritization and management
- Increasing engagement and collaboration

Performance Metrics

Total Portal Users:

8,153

7,707 Members

446 Partners

Total Organizations:

1,275

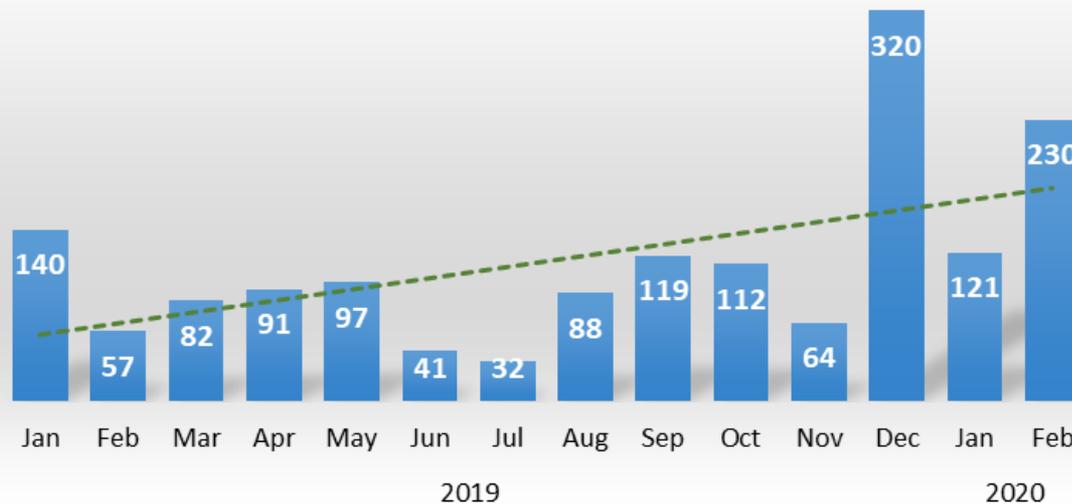
1,168 Members

107 Partners

Coverage:

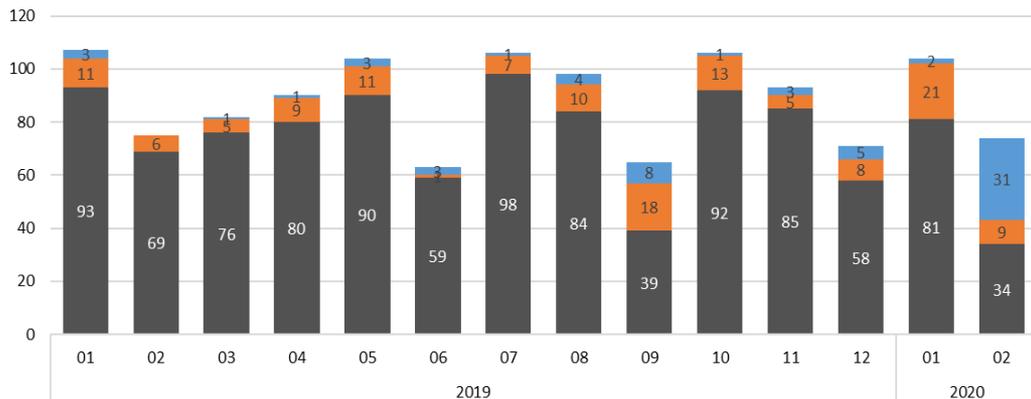
35% of utility orgs.
servicing \approx 75% of end
customers collectively

Members Added - Last 14 months



Member Voluntary Shares - Physical

■ Bulk ■ Portal-Main ■ Other



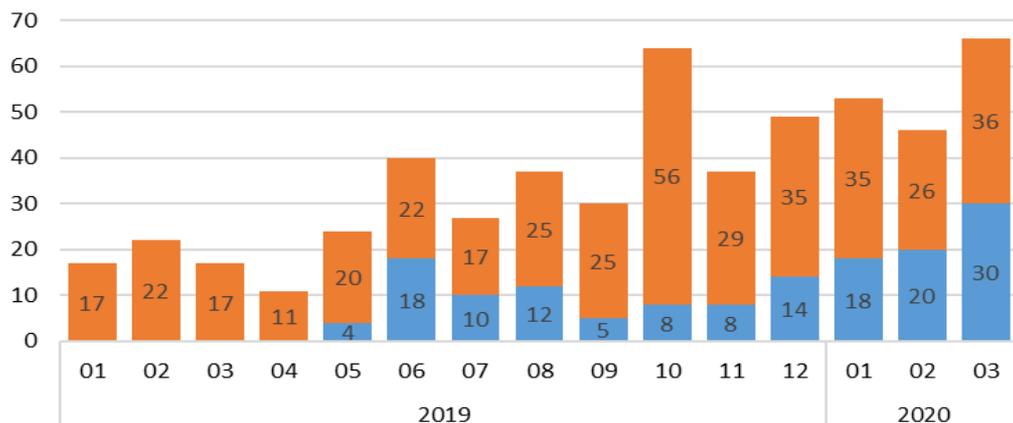
1,238

Physical

- 59 unique member organizations had at least one physical share (Jan'19-Feb'20)
- 81% of all shares came from two members
- Most sharing came outside of the Portal (via bulk)

Member Voluntary Shares - Cyber

■ Other ■ Portal-Main

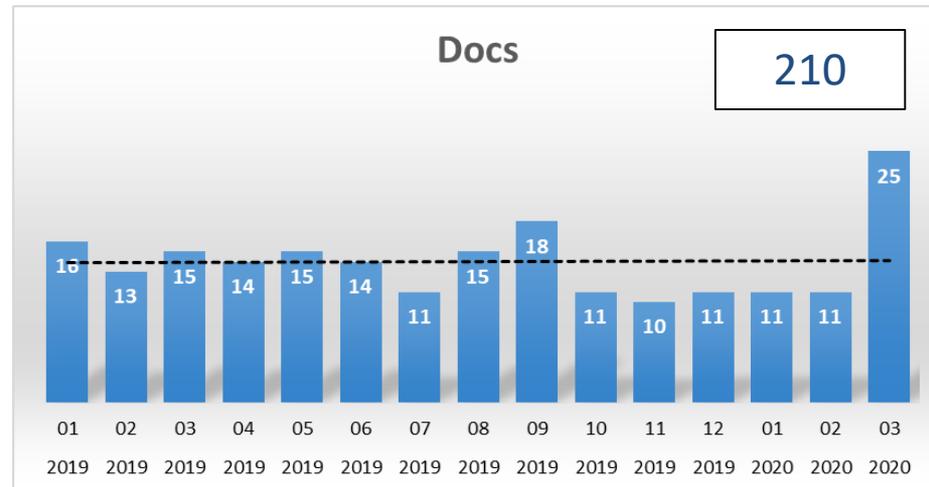
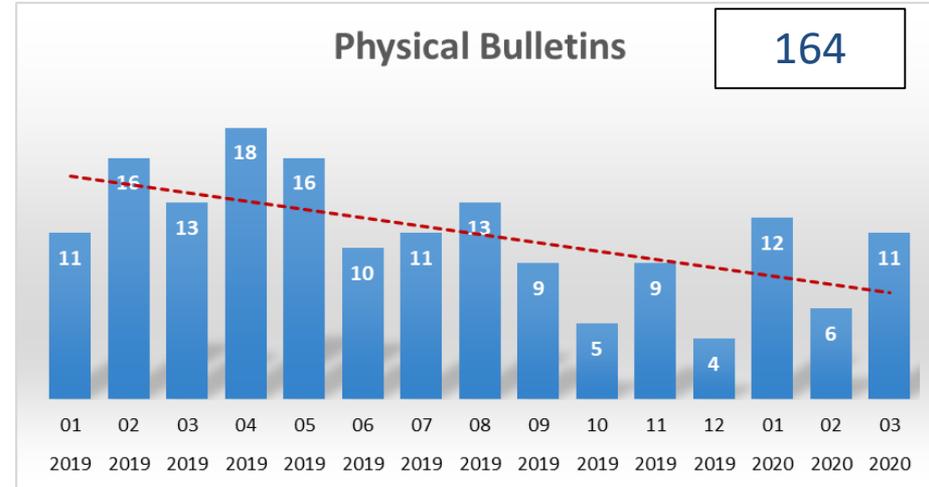
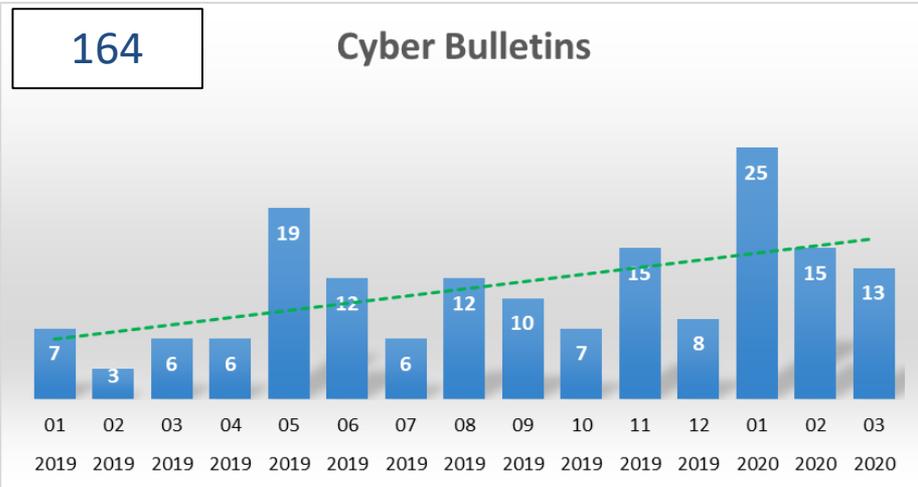


540

Cyber

- 101 unique member organizations had at least one cyber share (Jan'19-Mar'20)
- 9 members had 10 or more shares
- Most sharing came via the Portal, but other channels are increasing in use

E-ISAC Staff Portal Postings (Volume)





Questions and Answers

E-ISAC Preliminary 2021 Budget

Action

Review

Background

The objective of this agenda item is to present the E-ISAC's 2021 budget projection. The total 2021 E-ISAC budget projection is slightly below (-0.5%) the 2020 budget. The 2021 projection, excluding CRISP costs which are primarily funded by CRISP participants, is approximately 5 percent higher than the E-ISAC's 2020 budget. Compared to prior projections, the total 2021 direct cost projection, inclusive of CRISP costs, is approximately 9.5 percent below the projection presented in last year's budget. The non-CRISP budget projection is also significantly lower (approximately 8 percent) than the prior 2021 projection. This decrease is primarily due to lower than anticipated staffing requirements and increased efficiency of operations. These lower than previously projected resource needs are not expected to adversely impact the E-ISAC's ability to execute its mission, including support of near-term priorities.

Management will continue to evaluate options to further reduce direct costs. The 2021 projection will also be revised, if necessary, to account for the finalized CRISP budget, feedback from stakeholders, and other inputs. The final proposed budget will be presented to the ESCC Member Executive Committee in July for final review and endorsement prior to submittal to the Technology and Security and Finance and Audit Committees for review and recommendation to the Board of Trustees as part of NERC's overall 2021 budget.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Preliminary 2021 E-ISAC Budget

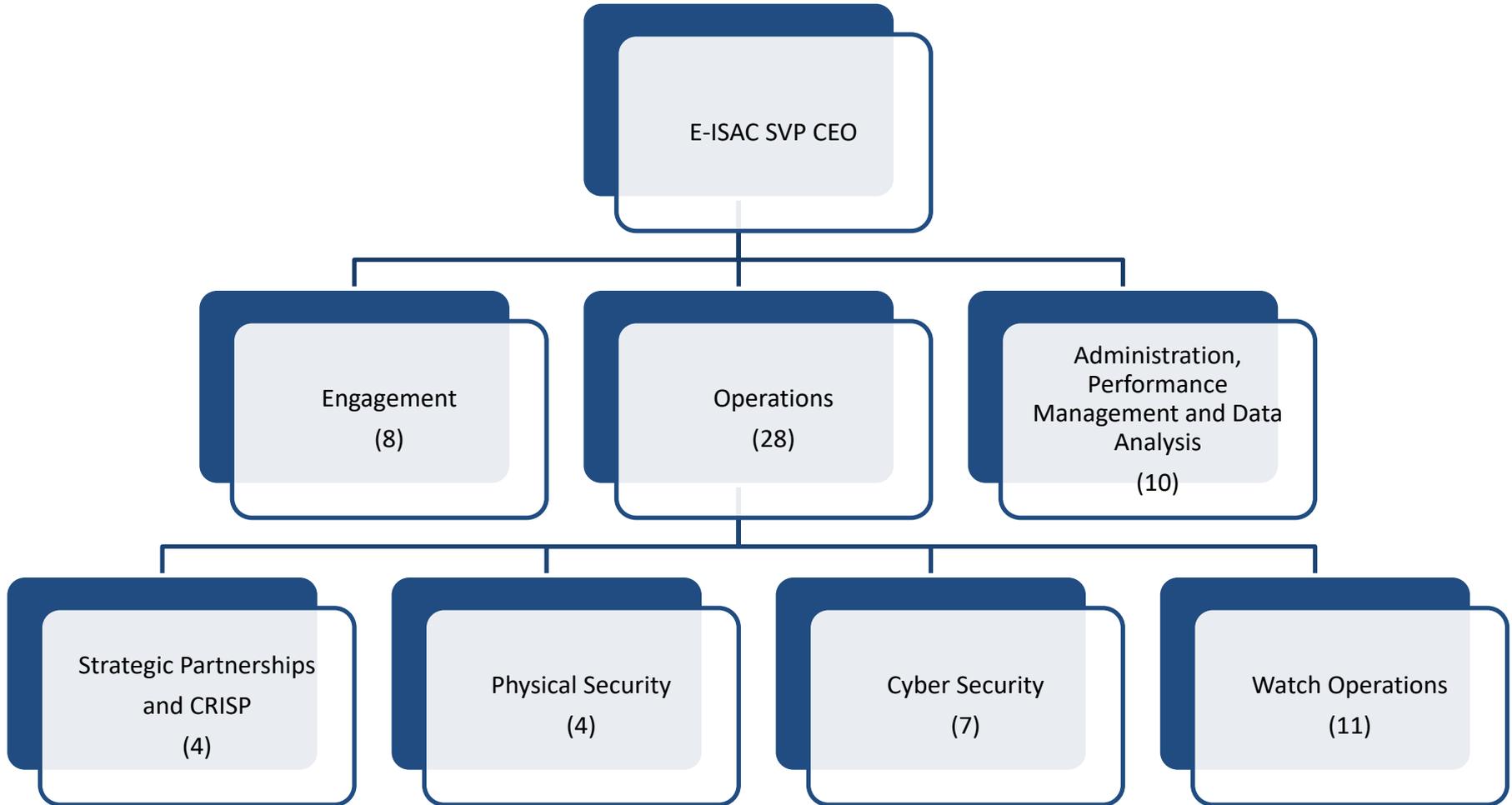
Andy Sharp, Vice President, Interim Chief Financial Officer
Technology and Security Committee Open Meeting
May 13, 2020

RELIABILITY | RESILIENCE | SECURITY



2019	2020	2021
On budget	On budget (projected)	Below prior projection

- Resource focus (2020-2021)
 - Supporting near-term strategic plan priorities
 - Reduction in projection is not expected to impact current initiatives
 - Mitigating upward resource pressure
 - Ensuring effectiveness and efficiency of operations
 - Maximizing utilization of current staffing, teamwork
 - Leveraging partnerships
 - Effective use of technology to support strategy



E-ISAC DIRECT COSTS
2021 Projection --- 2021 Revised Budget Projection

	2021 Projection from 2020 BP&B	2021 Revised Projection	\$ Change	\$ Change
Personnel	\$ 11,493,752	\$ 9,390,243		
Meetings & Travel	464,200	297,080		
Operating Expenses	9,844,202	9,927,042		
Fixed Assets	671,450	692,880		
Total Direct Costs	\$ 22,473,604	\$ 20,307,245	\$ (2,166,359)	-9.6%
CRISP Portion	\$ 8,311,450	\$ 7,556,059	\$ (755,391)	-9.1%
Non-CRISP Portion	\$ 14,162,154	\$ 12,751,186	\$ (1,410,968)	-10.0%

E-ISAC DIRECT COSTS 2020 Final Budget --- 2021 Revised Budget Projection

	2020 Final Budget	2021 Revised Projection	\$ Change	\$ Change
Personnel	\$ 9,825,628	\$ 9,390,243		
Meetings & Travel	464,200	297,080		
Operating Expenses	9,728,189	9,927,042		
Fixed Assets	421,450	692,880		
Total Direct Costs	\$ 20,439,467	\$ 20,307,245	\$ (132,222)	-0.6%
CRISP Portion	\$ 8,103,901	\$ 7,556,059	\$ (547,842)	-6.8%
Non-CRISP Portion	\$ 12,335,566	\$ 12,751,186	\$ 415,620	3.4%

- Total E-ISAC direct costs including CRISP slightly less than 2020 budget and \$2.2M (9.6%) below prior forecast
- E-ISAC direct costs excluding CRISP up \$416k (3.4%) over 2020 budget and \$1.4M (10.0%) below prior forecast
- Continue to evaluate options to reduce direct costs
- Cybersecurity Risk Information Sharing Program (CRISP)
 - Adjustments for known changes and expected lower PNNL costs
 - Participant costs declining primarily due to additional DOE funding
 - Budget, including operational technology pilot funding, subject to review with participants

- E-ISAC (excluding CRISP) 2021 projection summary – increase of \$416k (3.4%) over 2020 budget and \$1.4M (10.0%) below prior 2021 projection
 - Personnel:
 - Below prior projection by \$2.1M (20%) – lower FTE resources
 - Phased transition of watch contractors to full time employees
 - Ongoing evaluation of watch resource needs
 - Market increases in compensation and benefits
 - Operating Expenses
 - Above prior projection by \$823k (32%)
 - Continued contractor support for Watch operations during phased transition
 - Ongoing software, hardware, and contractor costs
 - Resource support for physical security threat workshops

- E-ISAC (excluding CRISP) 2021 projection summary (continued)
 - Fixed Assets
 - Flat with prior projection
 - Data platform, portal, and secure data center investments
 - Meetings, Travel and Conference Calls
 - Decreased by \$147k – meetings (30%) and travel (40%)

- **May-June:** Feedback and follow up with Member Executive Committee
- **July 14:** Second draft posted for comment
- **July 21 :** MEC conference call to review final proposed 2021 E-ISAC budget
- **July 23:** FAC webinar to preview second draft
- **August 20:** Final E-ISAC budget presented to NERC Board as part of overall NERC budget



Questions and Answers

ERO Enterprise Business Technology Projects Update

Action Update

Background

During the February 5, 2020 Technology and Security Committee (TSC) meeting, NERC provided an update on several ERO Business Technology topics, including:

- The status of the **Align** Project¹
- The status of the ERO Enterprise Secure Evidence Locker (**ERO SEL**)
- The status of the November release of the Centralized Organization Registration ERO System, the consolidated entity registration system enhancement
- The status of version 3 of the Situation Awareness for FERC, NERC and the Regional Entities
- The status of technology projects for the Electricity Information Sharing and Analysis Center (E-ISAC), including the Salesforce customer relationship management tool, the E-ISAC Portal, and the E-ISAC Data Analysis Platform.

Summary

NERC Information Technology continues in its mission to deliver technology solutions supporting the effective and efficient use of resources for registered entities and across the ERO Enterprise.

Since the February meeting, NERC has continued to progress in the development of the Align tool and the ERO SEL. NERC, however, expects to delay implementation of Phase 1 of the Align tool (focused on registered entity self-reporting and mitigation of noncompliance) and the ERO SEL until Q1 2021. The delay will allow for fulsome discussion on the May 14, 2020 Board conference call and accounts for potential delays that could result from supply chain disruption due to the coronavirus health crisis. The second and third releases for the Align tool project are expected by the end of 2021. Additional information on the Align tool and the ERO SEL is provided in the material for the agenda items 4 and 5, respectively.

¹ The Align Project (previously referred to as the CMEP Technology Project) is a strategic initiative designed to support the ERO Enterprise as it continues to evolve as a risk-informed regulator. It supports three ERO Enterprise goals: implementation of a risk-informed CMEP (Goal 2), reduction of known risks to reliability (Goal 3), and improving the efficiency and effectiveness of the ERO (Goal 6).

ERO Enterprise Align Project Update

Action Update

Background

At its February 5, 2020 Technology and Security Committee (TSC) meeting, NERC provided an update on the status of the Align Project. Since the February meeting, NERC has continued to progress in advancing the project, as discussed below.

The Align Project resulted from the strategic efforts of the ERO Enterprise, beginning in 2014, to improve and standardize processes across the ERO Enterprise for the Compliance Monitoring and Enforcement Program (CMEP). As the ERO Enterprise continues to mature its risk-based approach for the CMEP, it is imperative that the ERO Enterprise develop a more comprehensive and secure system to manage and analyze information.

Currently, each Regional Entity and NERC executes the CMEP, supported by largely homegrown systems and evidence collection practices.¹ As a result, registered entity experience differs across the country and the range in Regional Entity practices has frustrated multi-regional registered entities.

To address these issues, the ERO Enterprise is developing the Align tool and the ERO Enterprise Secure Evidence Locker (ERO SEL). These tools will provide a platform to enable harmonization of Regional Entity practices driving to a common registered entity experience. To date, 53 CMEP processes have been harmonized and that work is ongoing. These efforts are also enabling harmonization of documentation practices particularly as they relate to content of work papers. Additional information about the ERO SEL is provided in the background material associated with TSC Agenda Item 5.

The Align tool is a work and data management system built from a governance, risk, and compliance platform. When implemented, it will be used to manage all ERO Enterprise developed work products associated with CMEP activities. It will integrate with the Centralized Organization Registration ERO System (CORES), the consolidated entity registration system enhancement, and includes a repository of Reliability Standards.

¹ One of two “backbone” systems unifies these systems. Four Regional Entities use one system, provided by OATI, and a second custom-built system is used by two other Regional Entities, supplemented by auditor developed spreadsheets and word documents for data collection and organization. Regional work products are then “synced” with a NERC-owned system for oversight and reporting purposes. Furthermore, evidence is collected and managed in differing ways with tools that have different security postures. Registration systems exist outside of the CMEP, as does the Reliability Standards repository. Therefore, these two systems are individualized for each Regional Entity.

In 2018, NERC selected a vendor for the Align tool. During the development process, in mid-2019, NERC paused the project to evaluate the impact of the sale of the vendor designing the Align tool to a private equity firm. After significant forensic work and additional information gathering, NERC concluded that the risks associated with the vendor's upstream ownership could be effectively managed through a combination of technical and process controls rather than relying on vendor ownership as a control. These controls include data encryption, access controls (both user IDs and multi-factor authentication), dispersion of content, with evidence housed in a separate tool, and significantly enhanced work products. More importantly, part of the significant change management process associated with the implementation of the Align tool includes strict retention and destruction policies, and training on documentation of findings and work papers to prevent the duplication in those documents of sensitive information housed outside of the Align tool. NERC also intends to engage an independent third party to evaluate the final code to provide configuration management assurance that the Align tool is built as designed.

The Align tool, together with the ERO SEL, will provide the ERO Enterprise with a secure, effective, and harmonized platform with which to execute its CMEP responsibilities. These new tools will allow the retirement of existing legacy systems in use at NERC and the Regional Entities, substantially increase the security of registered entity data and ERO Enterprise work products, enable better oversight of Regional Entity processes, improve the quality and security of reporting, and provide substantial registered entity convenience with the integration to the Align tool (but not to the ERO SEL) of the CORES registry and the standards repository.

NERC expects to delay implementation of the Phase 1 Align release (focused on registered entity self-reporting and mitigation of noncompliance) and the ERO SEL until Q1 2021 to allow for fulsome discussion on the May 14, 2020 Board conference call, and to account for potential delays that could result from supply chain disruption due to the coronavirus health crisis.

Establishment of the ERO Enterprise Secure Evidence Locker

Action

Review and recommend to the Finance and Audit Committee.

Background

Pursuant to its mandate, the Technology and Security Committee (TSC) is charged with, among other things, providing the Finance and Audit Committee (FAC) and the Board of Trustees (Board) “with recommendations regarding management-proposed resource requirements and funding for the design, procurement, installation, operation, and maintenance of information technology hardware, software and applications, including hardware, software, and applications hosted by third parties, supporting NERC’s operations and program area initiatives.” Consistent with the mandate, NERC management requests that the TSC recommend to the FAC that the Board approve investment in the ERO Enterprise Secure Evidence Locker (ERO SEL).

Summary

As discussed further below, the ERO SEL would support the secure transfer, management, retention, and destruction of sensitive registered entity files used in Compliance Monitoring and Enforcement Program (CMEP) activities. It would complement the development of the Align tool, which is a work and data management system that the ERO Enterprise will use to manage all ERO Enterprise-developed work products used in CMEP activities. Collectively, the Align tool and the ERO SEL will provide a platform to enable harmonization of Regional Entity practices driving to a common registered entity experience while facilitating the secure submission, review, and retention of evidence generated during CMEP activities.

Both the ERO SEL and the Align tool resulted from the strategic efforts of the ERO Enterprise, beginning in 2014, to improve and standardize processes across the ERO Enterprise for the CMEP. As the ERO Enterprise continues to mature its risk-based approach for the CMEP, it is imperative that the ERO Enterprise develop a more comprehensive and secure system to manage and analyze information.

Currently, each Regional Entity and NERC executes the CMEP, supported by largely homegrown systems and evidence collection practices.¹ As a result, registered entity experience differs across the country and multi-regional registered entities have been highly frustrated by the range in Regional Entity practices. In addition, due to significant changes in the security landscape, there was an increased need to reevaluate the manner in which the ERO Enterprise protects critical data obtained during CMEP activities.

¹ One of two “backbone” systems unifies these systems. Four Regional Entities use one system provided by OATI and a second custom-built system is used by two other Regional Entities, supplemented by auditor developed spreadsheets and Word documents for data collection and organization. Regional work products are then “synced” with a NERC-owned system for oversight and reporting purposes. Furthermore, evidence is collected and managed in differing ways, with tools that have different security postures. Registration systems exist outside of the CMEP, as does the Reliability Standards repository. Therefore, these two systems are individualized for each Regional Entity.

To address these issues, the ERO Enterprise developed the Align tool and the ERO SEL, in addition to the Centralized Organization Registration ERO System (CORES). It is important to recognize that the CMEP evidence security issues underlying the need for the ERO SEL exist independent of the need to implement the Align tool. The security of evidence under the current mix of systems must be improved to meet an evolving security landscape. The ERO SEL is necessary under any circumstances; it is not simply a change to the Align project. Following is additional information on the ERO SEL.

As noted, the ERO SEL is designed to facilitate the secure submission, review, and retention of evidence generated in connection with CMEP activities. In short, all evidence provided by a registered entity would be required to be placed into either an ERO SEL or a registered entity locker that meets certain security criteria, unless prohibited by a Reliability Standard.² ERO Enterprise CMEP personnel would be able to view and analyze the evidence to perform their CMEP responsibilities.

Developing and implementing the ERO SEL will harmonize the evidence collection processes across the ERO Enterprise and establish the “gold standard” for security in this area. The ERO SEL would be hosted at NERC and designed as a stand-alone system. It will have no integration or network connection with the Align tool to increase security of both tools. Additionally, the proposed ERO SEL architecture and operational model will adhere to the NIST 800-171 security control framework, established to protect Controlled Unclassified Information (CUI) in nonfederal systems, wherein Critical Energy Infrastructure Information is classified as CUI.

Thus, the ERO SEL is designed to reduce risk significantly for evidence loss and exposure. It will have the following functionality and security:

- Enable submission by authorized and rigorously authenticated registered entity users;
- Provide compartmentalized analysis of evidence in temporary, isolated, and disposable environments;
- Prohibit interfaces with any other systems, including the Align tool;
- Encrypt immediately upon submission;
- Isolate submissions per entity;
- Prohibit extraction and backups; and,
- Prescribe proactive and disciplined destruction policies.

NERC’s use of virtualization technologies in the ERO SEL provides for an abstraction layer between server hardware and specialized use servers resulting in a one-to-many capability between hardware and server. This is an efficient and secure approach that meets the needs of the ERO SEL. Specifically, the design in conjunction with logical access controls implemented on the specialized use servers allows the Regional Entities to control their portion of the ERO SEL while NERC would perform the administrative functions.

² While the ERO will build and maintain the ERO SEL, Registered Entities may build, at their discretion, their own secure evidence lockers so long as they meet specified requirements for ERO Enterprise personnel access and data manipulation for analysis.

NERC Information Technology and the Project Management Office engaged Presidio—a long standing NERC vendor—to serve as a “general contractor” to design, build, implement, and service/maintain the ERO SEL. NERC is looking to complete this project and bring the ERO SEL online by the fourth quarter of 2020. In addition to designing and building the ERO SEL, NERC will purchase hardware and software that will be incorporated into the ERO SEL by Presidio. Presidio will also engage third-party subcontractors to assist throughout the project. NERC will engage a third party to verify the code for the system meets NERC’s specifications before launch.

As part of its outreach efforts and following a series of discussions with industry regarding the structure and functionality of the ERO SEL and Align tool. In April 2020, NERC presented details regarding the implementation process for the ERO SEL, related costs, and funding strategy. The ERO SEL represents an unbudgeted capital investment of \$3.8 million in 2020. Based on the latest financial projections available, NERC management proposes a combination of an operating contingency reserve draw of \$1.8 million and debt financing of \$2.0 million to fund the total ERO SEL capital investment in 2020. This approach will maintain annual debt service levels less than previous debt service projections in future years. NERC management also proposes drawing from operating contingency reserves in 2021 to fund the delay costs. In 2021, NERC is projecting a budget impact of \$770,000 for license, support, maintenance, certification and personnel costs to support the ERO SEL project.

NERC staff is seeking approval of the investment in the ERO SEL and its intended financing approach from the Board (preceded by review and recommendation by the TSC and the FAC) in May 2020. Upon Board approval, NERC will also seek approval from the Federal Energy Regulatory Commission of the associated budget variance for 2020 required to acquire and fund the ERO SEL.

NERC expects to delay implementation of the ERO SEL and Phase 1 of the Align tool (focused on registered entity self-reporting and mitigation of noncompliance) until Q1 2021 to allow for fulsome discussion on the May 14, 2020 Board conference call, and recognizing the potential delays that could result from supply chain disruption due to the corona virus health crisis.

The ERO SEL is a prudent and necessary response to the continuously evolving security landscape. Combined with the Align tool, the ERO SEL will provide the ERO Enterprise with a secure, effective, and harmonized platform with which to execute its CMEP responsibilities. These new tools will allow the retirement of existing legacy systems in use at NERC and the Regional Entities, substantially increase the security of registered entity data and ERO Enterprise work products, enable better oversight of Regional Entity processes, improve the quality and security of reporting, and, with respect to the Align tool’s integration with CORES registry and the standards repository, provide substantial efficiencies to registered entities.