

## Agenda

# Technology and Security Committee Meeting

August 16, 2023 | 8:30–9:30 a.m. Eastern

### **In-Person**

Westin Ottawa Hotel  
11 Colonel By Dr.  
Ottawa, ON K1N 9H4, Canada

**Conference Room:** Confederation I/II

### **Virtual Attendees**

[Webcast Link](#)

### **Introduction and Chair's Remarks**

[NERC Antitrust Compliance Guidelines](#)

### **Agenda Items**

- 1. Minutes\* – Approve**
  - a. May 10, 2023 Open Meeting
- 2. ERO Enterprise Business Technology\* – Update**
  - a. IT Solutions Customer Experience
- 3. E-ISAC Operations\* – Update**
  - a. E-ISAC Brief on the Threat Landscape
  - b. Member Executive Committee Summary
  - c. E-ISAC Customer Experience
- 4. Other Matters and Adjournment**

\*Background materials included.

## Draft Minutes Technology and Security Committee Open Meeting

Agenda Item 1a

May 10, 2023 | 10:00-11:00 a.m. Eastern

NERC DC Office  
1401 H Street NW, Suite 410  
Washington, DC 20005

### Call to Order

Ms. Jane Allen, Committee Chair, 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 May 10, 2023, at approximately 10:00 a.m. Eastern, and a quorum was declared present.

Present at the meeting were:

### Committee Members

Jane Allen, Chair  
Suzanne Keenan  
Robin E. Manning  
Jim Piro  
Colleen Sidford  
Kenneth W. DeFontes. Jr., *ex officio*

### Board Members

James B. Robb  
George S. Hawkins  
Robert G. Clarke  
Susan Kelly  
Kristine Schmidt

### NERC Staff

Tina Buzzard, Assistant Corporate Secretary  
Manny Cancel, Senior Vice President and CEO of the E-ISAC  
Kelly Hanson, Senior Vice President and Chief Administrative Officer  
Stan Hoptroff, Vice President, Business Technology  
Mark Lauby, Senior Vice President and Chief Engineer  
Bryan Preston, Vice President, People and Culture  
Sonia Rocha, Senior Vice President, General Counsel, and Corporate Secretary  
Andy Sharp, Vice President and Chief Financial Officer  
LaCreacia Smith, Senior PMO Manager (virtual)  
Angus Willis, Director of IT Core Infrastructure and Support (virtual)

### NERC Antitrust Compliance Guidelines

Ms. Allen directed the participants’ attention to the NERC Antitrust Compliance Guidelines included in the advance agenda package and indicated that all questions regarding antitrust compliance or related matters should be directed to Ms. Rocha.

**Chair's Remarks**

Ms. Allen welcomed participants to the meeting. She reviewed the agenda and reported on the recent closed meetings of the Committee.

**Minutes**

Upon motion duly made and seconded, the Committee approved the minutes of the February 15, 2023, meeting as presented at the meeting.

**Cyber Strategy**

Mr. Cancel began with a discussion of the recent cyber incident at a NERC vendor, Dragos, Inc. He noted that no NERC data was compromised in the incident and commended Dragos' response and transparency.

Mr. Cancel followed with a presentation on the recent reports and strategies released by the Canadian and U.S. governments. He discussed the (1) U.S. Office of the Director of National Intelligence (ODNI) Annual Threat Assessment, (2) Canadian Centre for Cybersecurity Threat Assessment, and (3) National Cybersecurity Strategy.

**E-ISAC Operations**

Mr. Cancel also provided an update on E-ISAC operations. His update included a discussion of the security threat landscape, new E-ISAC products and services; and activities with the Energy Threat Analysis Center (ETAC). The Committee and attendees discussed the ETAC pilots and governance, benchmarking against other sectors, the quantity of cyber events per year.

**ERO Enterprise Business Technology**

Mr. Hoptroff, along with Ms. Smith and Mr. Willis, provided updates on the Align tool, NERC's IT infrastructure services team, and NERC's use of the cloud. Ms. Smith reviewed lessons learned from Align implementation, Align financials, and the timeline of the completion of the Align tool and retirement of legacy applications. Mr. Willis provided an overview of the IT Infrastructure Services team. He also provided an overview of the drivers for and manner in which NERC currently uses cloud technology as well as NERC's plans to expand use of cloud technology in the coming years.

**Adjournment**

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

Submitted by,



Sônia Rocha  
Corporate Secretary

## **ERO Enterprise Business Technology**

### **Action**

Update

### **Background**

Management will provide an overview of NERC's approach to customer support for its business technology solutions and an update on adoption of Align in Canada.

- Customer Support: Management will discuss NERC's support philosophy, the mechanism for providing support, and its support focus areas in 2023 and longer term to enhance the customer experience.
- Align: Management will provide an update on implementation of Align in Canada. Align is in production in Ontario, Nova Scotia, Manitoba, Saskatchewan, and in development in Alberta and British Columbia.

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

Agenda Item 2

# ERO Enterprise Business Technology Update

Stan Hoptroff, Vice President, Business Technology  
Technology and Security Committee Open Meeting  
August 16, 2023

**RELIABILITY | RESILIENCE | SECURITY**




- NERC Business Technology (BT) Support Update
- Align Canada Project Update



## Support

**NERC**  
NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## NERC Helpdesk Ticket Submission System

 **Submit**

[\\* required fields](#) | [Home](#) | [Contact Us](#)

### Submit a new Ticket

<b>Title *</b> <input type="text"/>	<b>Region *</b> <input type="text" value="Select"/>	<b>Priority *</b> <input type="text" value="Medium"/>
<b>Service *</b> <input type="text" value="Select"/>		
<b>File Attachment</b> <i>(If you need to send multiple files, please create a single zip file)</i> <input type="button" value="Choose File"/> No file chosen		

### Your Personal Information

<b>Last Name *</b> <input type="text"/>	<b>First Name *</b> <input type="text"/>	<b>Email Address *</b> <input type="text"/>
<b>User ID</b> <input type="text"/>	<b>Phone *</b> <i>(Format: xxx-xxx-xxxx)</i> <input type="text"/>	<b>Company *</b> <input type="text"/>

### Description

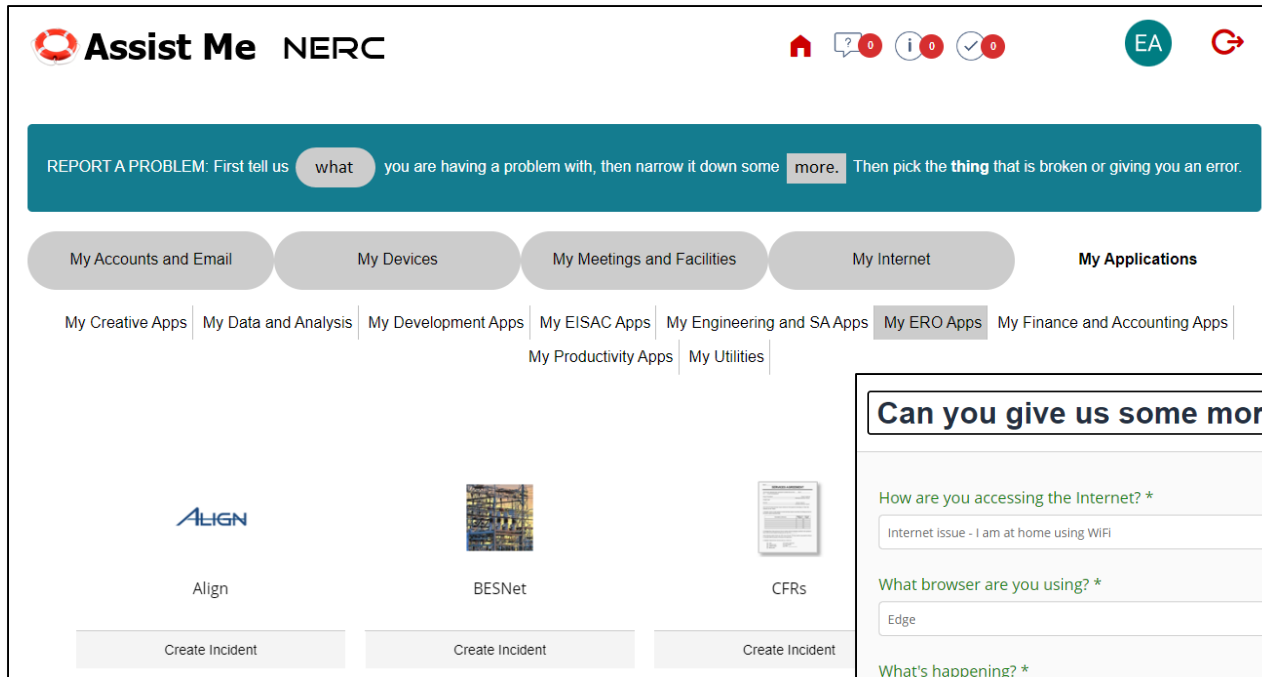
**Description \*** (1000 characters remaining)



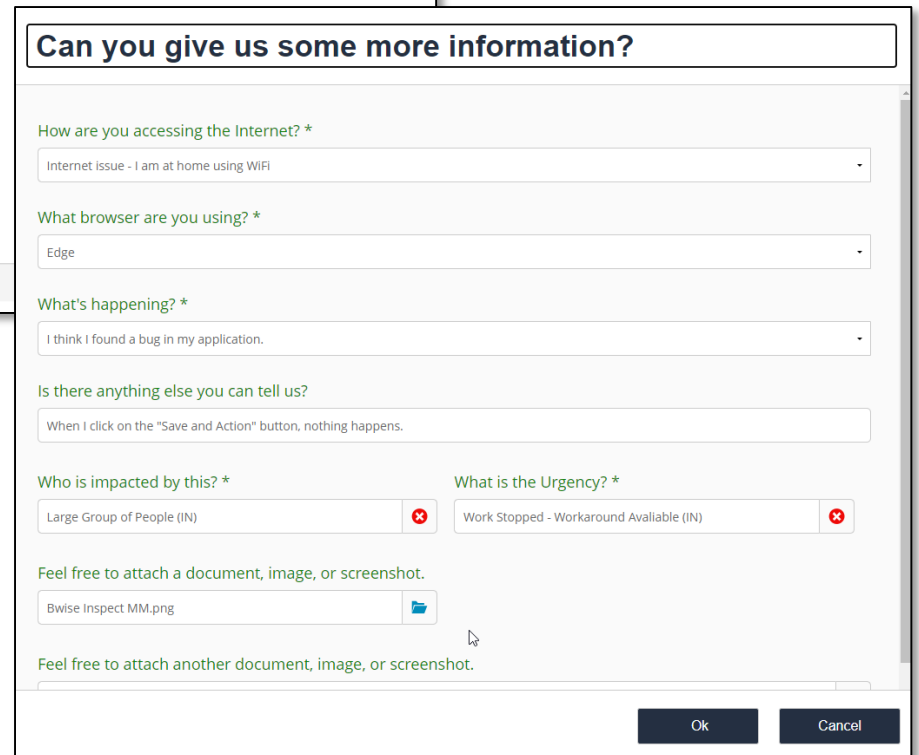
The screenshot displays the NERC Assist Me interface. At the top left is the 'Assist Me NERC' logo. The top right navigation bar includes a home icon, a help icon with a '0' notification, an information icon with a '0' notification, a checkmark icon with a '0' notification, an 'EA' icon, and a refresh icon. Below the navigation bar is a dark grey bar with the text 'News | Nothing new to report.' and navigation arrows. The main content area features three large, colored cards:

- I NEED SOMETHING...** (Green card): Includes a plus icon, the text 'Need us to install something? Give access? Provide training? Send you something? Just ask!', and an 'ASK US' button.
- SOMETHING IS WRONG!** (Teal card): Includes a warning icon, the text 'Error Message? Blank screen? No green lights? Don't worry - we'll get you taken care of.', and a 'TELL US' button.
- WHAT'S MY STATUS?** (Dark Blue card): Includes an eye icon, the text 'See your tickets and their status. Give us more information. Tell us how we did.', and a 'SHOW ME' button.

- Security is Priority Number One - *Monitor, Control, and Protect*
- Develop and Enhance Client Relationships
- Help People Help Themselves - *Self-Service and Online Help*
- Operational Excellence – *Focus on continuous improvement by leveraging our Quality Assurance Team*
- Learn from Others – *By using The Information Technology Infrastructure Library (ITIL)*
- Wisdom Through Data - *Analytics, Reporting, Feedback for Improvement*
- Embrace Simplicity - *Focus on Fundamentals*



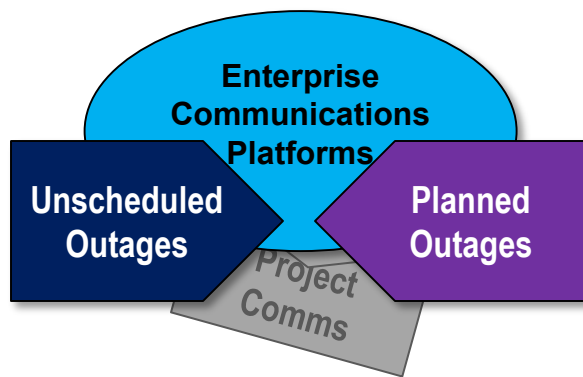
- Point and Click Visual Interface



- Up-Front Information Collection to Aid in Troubleshooting

## Transitioning Align and Secure Evidence Locker projects into Day-to-Day Operations

- Retooling support model and team structure for ongoing operations
- Onboarding and training additional staff for Level 1 Success Team, Level 2 Application Support, Level 3 Application Development



- Move from Project Change Management Communications into Operations Announcements

## Continuing IT Organizational Maturation

- Reviewing and Aligning with the IT Infrastructure Library (ITIL)
- Refining Policies, Procedures, and Internal Controls
- Knowledge Management and Documentation
- Measuring our Performance
- Reduce Outage Duration and Frequency

## **Continuing IT Organizational Maturation**

- Analytics and Operational Awareness
- Service Level Objectives
- Change Management Automation

## Align

- Enforcement Processing
- Canadian Regulator Access
- Audits, Spot Checks, and Scheduling
- Self-Reports
- Notifications
- Periodic Data Submittals and Self-Certifications
- Reports and Dashboards



- In Production: Ontario, Nova Scotia, Manitoba, and Saskatchewan
- Development In Progress: Alberta, British Columbia
- Quebec: Expressed interest in using Align
- New Brunswick: To be determined

- Focus on Enhancement Log
- Prioritization Based Upon:
  - System Functionality
  - User/Stakeholder Experience
  - Productivity Efficiencies



# Questions and Answers

- The ITIL framework is used to manage IT services effectively throughout the entire service lifecycle. ITIL provides guidelines and best practices for implementing the five phases of the IT service lifecycle: **strategy, design, transition, operations, and continual improvement**

## **E-ISAC Operations**

### **Action**

Update

### **Background**

The Electricity Information Sharing Analysis Center (E-ISAC) will provide an overview of cyber and physical security threats and E-ISAC responses to these threats; share feedback from the recent E-ISAC membership survey; and provide an update on the Vendor Affiliate Program.

### **Summary**

The threat environment continues to be dynamic, and the E-ISAC works closely with its partners to understand the threat, develop mitigations, and share best practices. The E-ISAC will present an updated view on what the threats to the electricity industry are, and how utilities can defend against them.

In addition, the E-ISAC received feedback from its members and partners about the quality of the products the E-ISAC develops, current services offered, and the overall satisfaction they have with the organization. This information informs the E-ISAC about the opportunities to enhance products and services, and ways in which the organization can best serve its members.

Finally, the E-ISAC will provide an update on the Vendor Affiliate Program, which is focused on facilitating information sharing and best practices in a trusted environment between vendors and E-ISAC member and partner organizations.



# E-ISAC Operations

Manny Cancel, NERC Senior Vice President and E-ISAC CEO  
Matthew Duncan, Director, Intelligence  
Bluma Sussman, Director, Membership  
Technology and Security Committee Open Meeting  
August 16, 2023

**TLP:CLEAR**

**RELIABILITY | RESILIENCE | SECURITY**



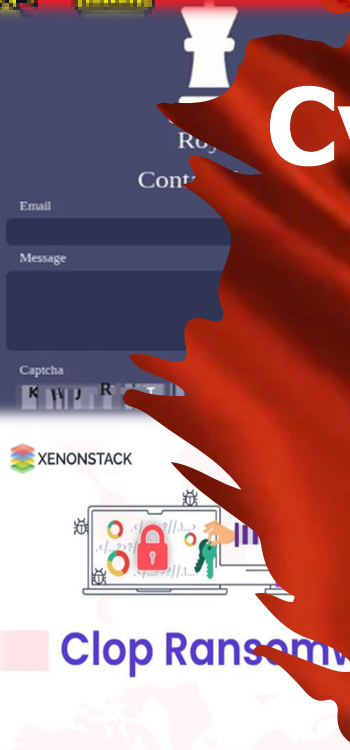


- Threat Landscape
  - Cyber Threats and Response
  - Physical Threats and Response
  - Collective Defense Actions and Considerations
- E-ISAC Membership and Survey Results
- Vendor Affiliate Program
- GridSecCon 2023
- GridEx VII



**LOCKBIT 3.0**

**BLACK BASTA  
RANSOMWARE**



# Cyber Threats and Response





- **China**

- Volt Typhoon targeting U.S. utility and other critical infrastructure sectors
- Storm-0558 hacks U.S. Commerce and State Departments
- Continued exploitation of MS Cloud, Citrix, Fortinet, VMware, Log4j vulnerabilities
- Improved tradecraft and evasion techniques

- **MOVEit File Transfer Supply Chain Compromise**

- Cl0p ransomware gang extortion campaign
- U.S. Government and Service Providers impacted

- **Prominent Vulnerabilities**

- Barracuda Email Security Gateway replacement advisory
- Fortinet Fortigate SSL-VPN
- Rockwell Automation ControlLogix Communication Module

- **Services**

- Analytic collaboration with ETAC and cross sector ISACs
- Threat hunting in CRISP data
- Monitoring of Dark Web, criminal forums, social media
- Outreach to members with vulnerable devices on internet
- E-ISAC CIOp MOVEit victim list
- Separate monthly briefings for members and regulatory partners

- **Products**

- All-Points Bulletins (Volt Typhoon, IBM Maximo)
- Critical ICS and IT vulnerabilities reports
- Cyber Threat Intelligence reports with mitigations
- Monthly ICS threat and trends report
- Weekly ransomware report
- Weekly Small and Medium Utility Community reports

- Meetings with Office of the National Cyber Director
- Finalizing governance
- Drafting processes and procedures
- Active analyst collaboration
  - Volt Typhoon
  - Ransomware
  - Operational Technology vulnerabilities
  - Snap calls on emerging threats
  - Analyst exchanges with DOE and labs

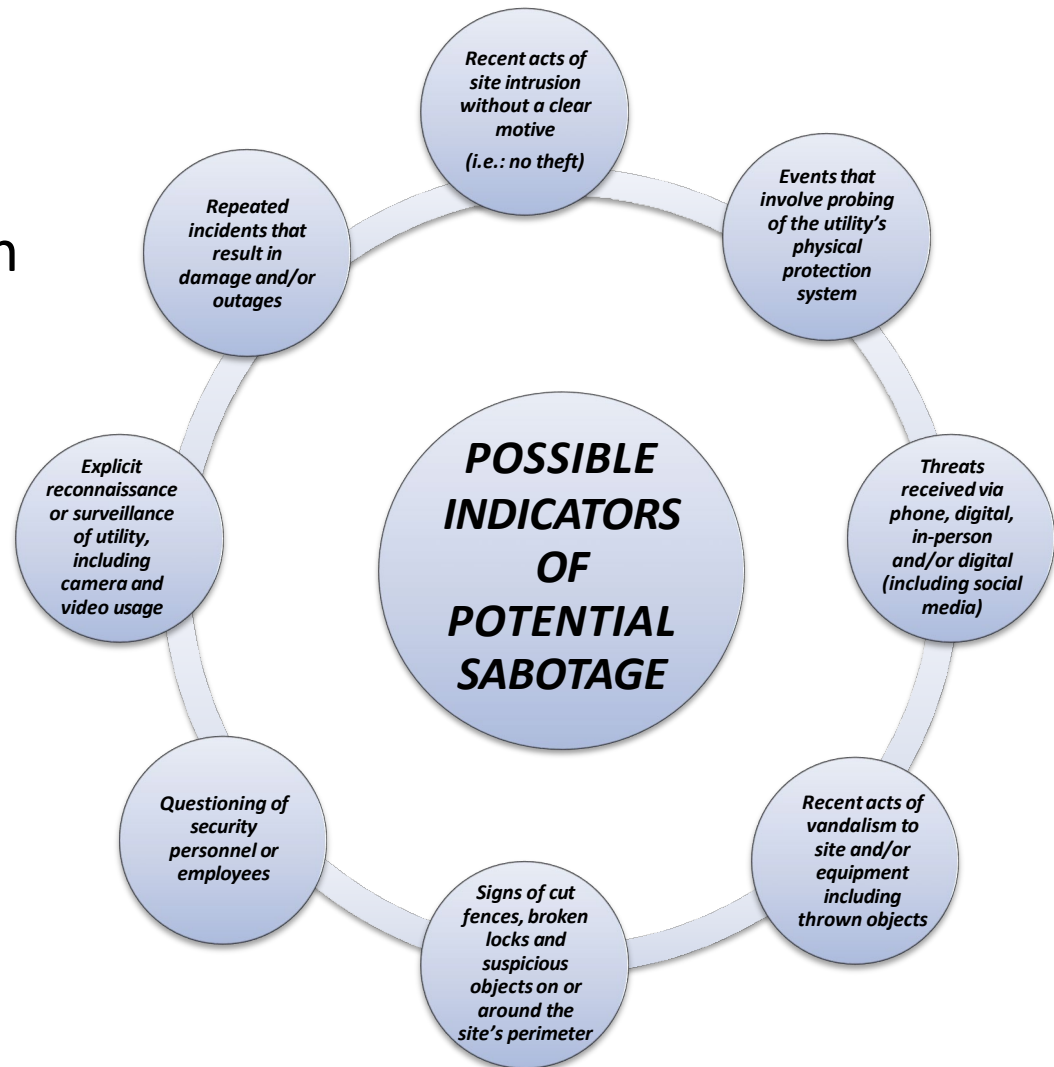


- 2020-2022: [E-ISAC Physical Security Report: Grid-Impacting Incidents \(2020-2022\)](#)
  - Of the physical security incidents shared with E-ISAC between 2020-2022, 97% resulted in no grid impact and 3% resulted in outages or other grid impacts
  - Notable increase in Q3-4 2022 compared to baseline trends over the previous 18 months
- 2023 Observations (thus far): [E-ISAC Physical Security Quarterly Report, Q1 2023](#)
  - Overall, the number of grid impacting (Level 2/3) incidents have decreased from Q4 2022, but are still elevated compared to historical numbers
  - Level 2/3 incidents in 2023 have involved similar types of tactics as seen in Q4 2022: vandalism, intrusion (tampering), ballistic damage, and theft



- Regular engagement with members, partners, and stakeholders
  - Intelligence community classified briefings
  - Cross-sector collaboration
  - Threat assessments
  - Joint tri-sealed products (JCAT First Responder's Toolbox: Electric Power Substation Terrorist Threat Awareness, Detection, and Initial Post-attack Response Consideration)
- E-ISAC mitigation tools and resources
  - Physical Security Resource and Risk Management Guide
  - Identifying Possible Avenues of Approach and Firing Positions at Substations
  - Online Threat Monitoring Report
  - Drone Detection Pilot
  - White Papers (UAS, Copper Theft, and Wind Farm Security)
  - Design Basis Threat and VISA Workshops

- Focus on physical security mitigation strategies and the Electricity Sector Design Basis Threat
- Take Incidents Seriously...
  - Examine the (potential) crime scene
  - Leverage information sharing: LLE/State Fusion Centers, FBI, E-ISAC, etc.
  - Practice continued vigilance
  - Insider Threat Mitigations





- **Share with E-ISAC and government/law enforcement**
  - Connect to E-ISAC and government automated sharing
  - Ensure compliance organization facilitates not hinders sharing
- **Deploy Internal Network Security Monitoring (INSM)**
  - Deploy INSM in critical OT networks and share data and analytics
- **Ensure cyber security informs supply chain procurement, operations, and contract language**
  - Ensure disconnection plans in place if a vendor is compromised
  - Ensure compromise disclosure requirements embedded in contract language
  - Ensure new renewable generation is secure by design



- Canadian Membership Summary
  - 69 member and 12 partners
  - 35 out of 42 Electricity Canada members
- 2023 Additions
  - Members: 7
  - Partners: 2



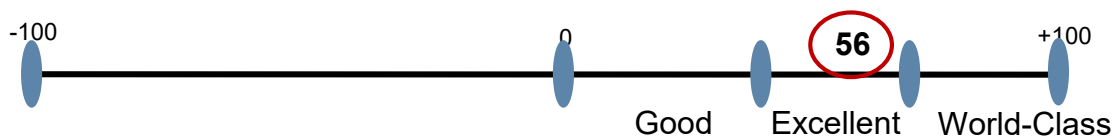
- 2023 Stakeholder Feedback Survey
  - Conducted in partnership with JD Power
  - Distributed to 8,039 individual Portal users
  - 14% Response Rate for organizations
    - 211 member and 35 partner organizations responded
    - Total number of responses: 356 individuals, up by 13% from 2021
- Survey Goals and Objectives
  - Gather feedback on stakeholder experience, products, and services
  - Identify best practices and areas for improvement
  - Included many 2021 survey questions, with some adjustments
  - Ability to draw comparisons between 2021 and 2023
  - Greater ability this year to analyze data



# E-ISAC 2023 Net Promoter Score

# 56

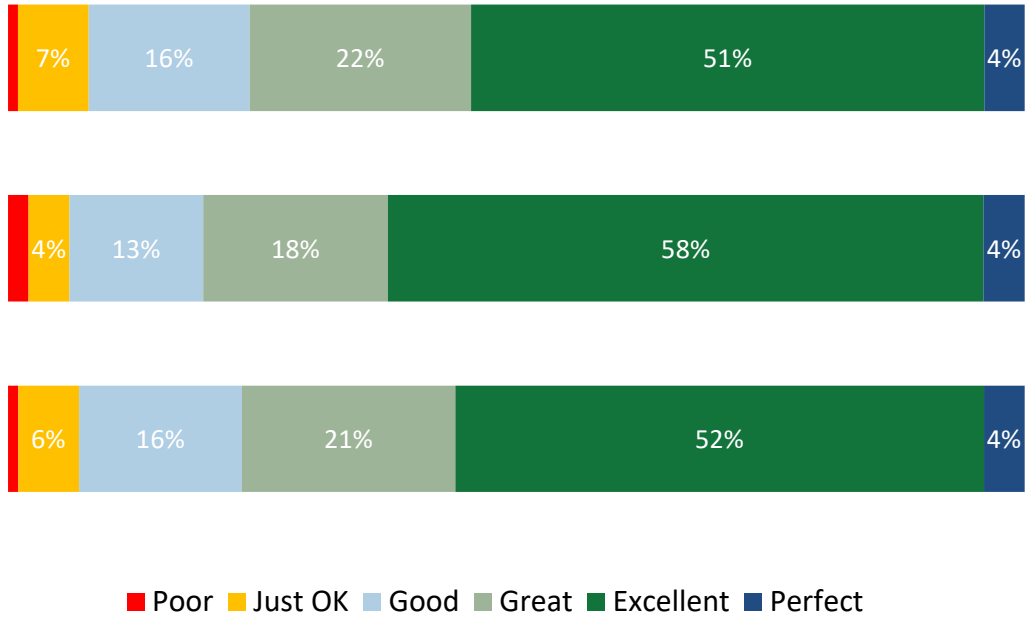
- What is a Net Promoter Score?
  - Widely used market research metric
  - Measures customer experience and loyalty
  - Ranges from -100 to 100
  - Scores above “0” are considered good





## Overall Satisfaction (OSAT)

Organization Record Type	2023 OSAT	Shift in "Excellent" Satisfaction vs. '21
Member	6.5 ↑	+7
Partner	6.8 ↑	+20
Overall	6.6 ↑	+9



**Scale:** 0 - 10

**Approach:** Poor = 0, Just OK = 2, Good = 4, Great = 6, Excellent = 8, Perfect = 10

**Calc:** % of respondents x rating weight

- 95% of members said information provided by the E-ISAC contributes to and/or increases their organization's security posture
- 98% of partners said participating in E-ISAC information sharing provide value to their stakeholders
- Most relevant products to members and partners\*:
  - All-points bulletins regarding ongoing attacks against electric infrastructure
  - Monthly Security Outlook on physical security trends
  - Online threat analysis reports
- Areas for further exploration
  - Timing of future surveys to increase response rate

\*Based on sample of products in survey



- Increase awareness of products
- Provide clear call to action and quality writing and analysis for products
- Focus on making products timely and actionable (products are already considered highly relevant)
- Maintain engagement with more tenured members

- Vendor Affiliate Program Year-1 Goals Achieved
  - 10 Vendor Organizations
  - \$200,000 in membership fees
  - Self-funding program
- Q2 shift from program launch to implementation; building thought leadership through:
  - Vendor presentations on E-ISAC Monthly Briefing
  - Vendor Industry Engagement Program
  - Collaboration with the CSAG
  - Participation in GridSecCon and GridEx
- Q3-Q4 focus on sustained engagement, growth, and retention

DRAGOS

FORTINET

NOZOMI  
NETWORKS

SIEMENS  
energy

1898  
CO

axio

FINITE STATE

Hitachi Energy

Sargent & Lundy

SEL SCHWEITZER  
ENGINEERING  
LABORATORIES

# GRIDSEC CON 2023

NERC • E-ISAC • NPCC

- Registration is [open](#)
- Two hotel options: [Hilton Québec City Hotel](#) and [Delta Québec](#)
- General Sessions, Keynotes, and Panels
- 10 training sessions and 24 breakout sessions
- For more information or sponsorship inquiries, please contact [events@eisac.com](mailto:events@eisac.com)

- Distributed Play (E-ISAC members/partners), November 14–15:
  - Distributed exercise materials
  - Completing training webinars
- Executive Tabletop (invitation only), November 16, 2023:
  - Trusted Agent meetings
  - Prep sessions with key participants
  - Hot wash on November 17
  - GridEx VII Lessons Learned Report – Q1 2024
  - Recommendations Review – Q2 2024



A map of North America is shown in a light blue color. A darker blue horizontal band runs across the middle of the map, passing through the United States. The text 'Questions and Answers' is centered within this band.

## Questions and Answers

## VISA overview:

- Cost-effective methodology
- Relies on subject matter expert input to determine overall system effectiveness
- Promotes developing sound business case to make informed risk-based decisions
- Provides confidence that a threat can be mitigated
- Helps utilities produce a portfolio of scenarios to justify upgrades
- View VISA workshop promotional video [here](#)

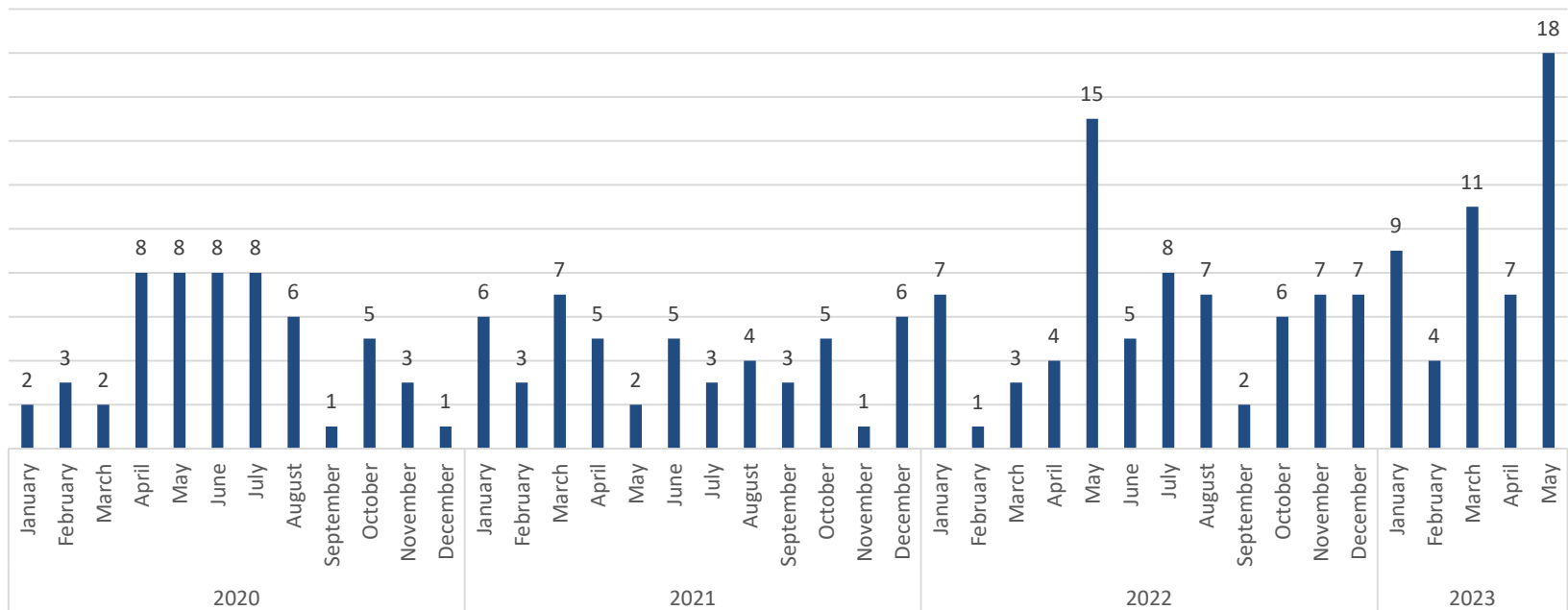
## VISA stats:

- 18 workshops since 2017
- 7 workshops in 2023
- 75% increase in number of workshops held from 2022 to 2023

## What's next:

- Identify options to support increased demand over next 5 years

- Continue to trend in elevated numbers in 2023 compared to historical incidents
- Most concerning tactics include ballistic targeting of substation transformers and switches (most likely to cause outages and heavy damages)
- Most common assets targeted include transmission assets (e.g., conductors, insulators, and structures) followed by substations (e.g., power transformers, voltage control equipment, and circuit breakers)



**Number of Ballistic Damage Incidents Shared Monthly Since 2020**