NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda
Technology and Security Committee Meeting

May 7, 2025 | 11:00 a.m.-12:00 p.m. Eastern
Hybrid Meeting

In-Person (Board, MRC, NERC Staff ONLY)

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

Virtual Attendees *(including presenters)*
Webinar Link: Join Meeting
Attendee Password: Day1ATTMay725 (32912886 from phones)
Audio Only: 1-415-655-0002 US | 1-416-915-8942 Canada| Access Code: 2309 991 0780

Committee Members
Jane Allen, Chair
Larry Irving
Susan Kelly
Jim Piro
Suzanne Keenan, *ex-officio*

Introduction and Chair's Remarks

NERC Antitrust Compliance Guidelines

Agenda Items

1. Minutes — **Approve**
   a. February 12, 2025 Open Meeting*
2. Business Technology Strategy* — **Update**
3. E-ISAC Operations *— **Update**
4. Other Matters and Adjournment

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Draft Minutes
Technology and Security Committee
Open Meeting

February 12, 2025 | 8:30-9:30 a.m. Eastern

In-Person
JW Marriott Miami
1109 Brickell Ave
Miami, FL 33131

Call to Order

Mr. Jim Piro, Committee member, 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 12, 2025, at approximately 8:30 a.m. Eastern, and a quorum was declared present.

Present at the meeting were:

Committee Members
Larry Irving
Suzanne Keenan
Susan Kelly
Robin E. Manning
Jim Piro
Kenneth W. DeFontes. Jr., *ex officio*

Board Members
Robert G. Clarke
George Hawkins
Colleen Sidford
Kristine Schmidt
James B. Robb, President and Chief Executive Officer

NERC Staff
Tina Buzzard, Assistant Corporate Secretary
Manny Cancel, Senior Vice President and CEO of the E-ISAC
Mathew Duncan, Vice President, E-ISAC Security Operations and Intelligence
Shamai Elstein, Associate General Counsel
Howard Gugel, Vice President, Regulatory Oversight
Kelly Hanson, Senior Vice President and Chief Operating Officer
Fritz Hirst, Vice President, Government Affairs
Stan Hoptroff, Vice President, Business Technology
Soo Jin Kim, Vice President, Engineering and Standards
Mark Lauby, Senior Vice President and Chief Engineer
Kimberly Mielcarek, Vice President, Corporate and External Communications
Sonia Rocha, Senior Vice President, General Counsel, and Corporate Secretary
Liz Saunders, Vice President, People and Culture
Andy Sharp, Vice President and Chief Financial Officer
LaCreacia Smith, Director, Project Management Office
Bluma Sussman, Vice President, E-ISAC Stakeholder Engagement

NERC Antitrust Compliance Guidelines

Ms. Buzzard 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

Mr. Piro welcomed participants to the meeting and reviewed the agenda. On behalf of Jane Allen, Committee chair, Mr. Piro thanked Mr. Hoptroff for his contributions and leadership.

Minutes

Upon motion duly made and seconded, the Committee approved the minutes of the August 14, 2024, open meeting as presented at the meeting.

ERO Enterprise Business Technology Strategic Plan

Ms. Smith provided an update on the implementation of the ERO Enterprise Business Technology Strategic Plan. She reported on the technology investments and solutions completed in 2024 and planned for 2025. The Committee discussed the new NERC website, the Reliability Coordinator Information System, and plans for continued solicitation on customer feedback on new deployments.

ERO Enterprise Stakeholder Engagement

Mr. Hoptroff provided an overview of the results of the 2024 ERO Enterprise Business Technology client survey. He noted that the purpose of the survey is to assess customer satisfaction with the Business Technology department and identify areas for continued improvement. Mr. Hoptroff reported that survey indicated that satisfaction with NERC's Business Technology improved from 2023 (in both customer support and Business Technology overall) and highlighted the following key areas for continued improvement: (1) ease of reporting issues; (2) notification to customers on status of reported issues; (3) speed of issue resolution; and (4) ensuring responses resolve the reported issue.

Threat Landscape

Mr. Duncan summarized the E-ISAC's recent activities and the threat landscape facing the electric industry, with a focus on a brief discussion of the incidents over the holiday season, Chinese cyber activity, and drones. He also provided a comparison of 2024 and 2023 cyber and physical direct shares, a proactive E-ISAC program to address visible vulnerabilities. The Committee discussed sharing with other Information Sharing and Analysis Centers and the Cybersecurity Risk Information Sharing Program.

E-ISAC Customer Experience

Ms. Sussman reported on the upcoming strategic implementation phase of the E-ISAC's stakeholder experience effort, reviewing information consumption, event participation, stakeholder sentiment factors, and plans to operationalize this feedback in E-ISAC products and services. The Committee discussed the use of personas to chart the stakeholder experience and the ability to customize the portal based on those personas.

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

Submitted by,

Sônia Rocha
Corporate Secretary

Agenda Item 2
Technology and Security Committee
Open Meeting
May 7, 2025

Business Technology Strategy

Action

Update

Summary

Management will provide an update on the implementation of the ERO Enterprise Business Technology Strategic Plan. The presentation will focus on critical 2026 business technology investments, as follows:

- Agility and Sustainability – Focus on foundational and specialized platforms, infrastructure upgrades, and operational excellence.
- *Engagement* – Focus on stakeholder engagement and outreach solution, System Operator Certification database, and data modeling for ERO enterprise analytics.
- *Energy* – Focus on data collection for inverter-based resources, cold weather data collection, and reliability assessment database.
- *Security* – Focus on additional cloud security capabilities and enhanced cyber security for data protection.

Management will also discuss the critical skills necessary for implementation of the strategic plan and potential implementation challenges.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Business Technology Strategy

Todd Carter, Vice President, Business Technology
Technology and Security Committee Open Meeting
May 7, 2025

RELIABILITY | RESILIENCE | SECURITY

Agenda

Critical 2026 Business Technology Investments

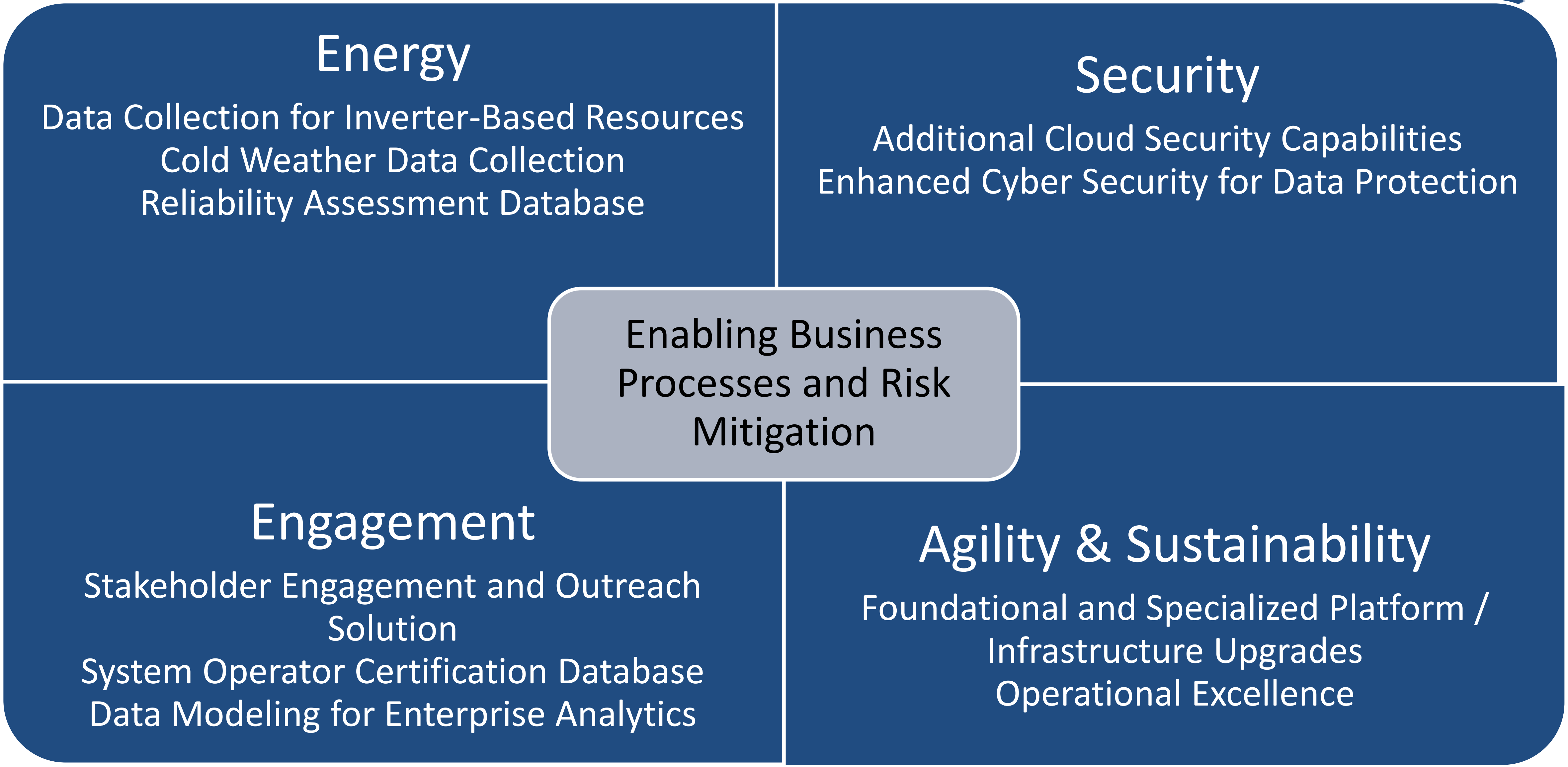
Retain and Develop Critical Skills

Challenges

Value Proposition of Technology Investments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical 2026 Business Technology Investments



Energy

Data Collection for Inverter-Based Resources
Cold Weather Data Collection
Reliability Assessment Database

Security

Additional Cloud Security Capabilities
Enhanced Cyber Security for Data Protection

Enabling Business Processes and Risk Mitigation

Engagement

Stakeholder Engagement and Outreach Solution
System Operator Certification Database
Data Modeling for Enterprise Analytics

Agility & Sustainability

Foundational and Specialized Platform / Infrastructure Upgrades
Operational Excellence

Retain and Develop Critical Skills

Cyber Security

Artificial Intelligence

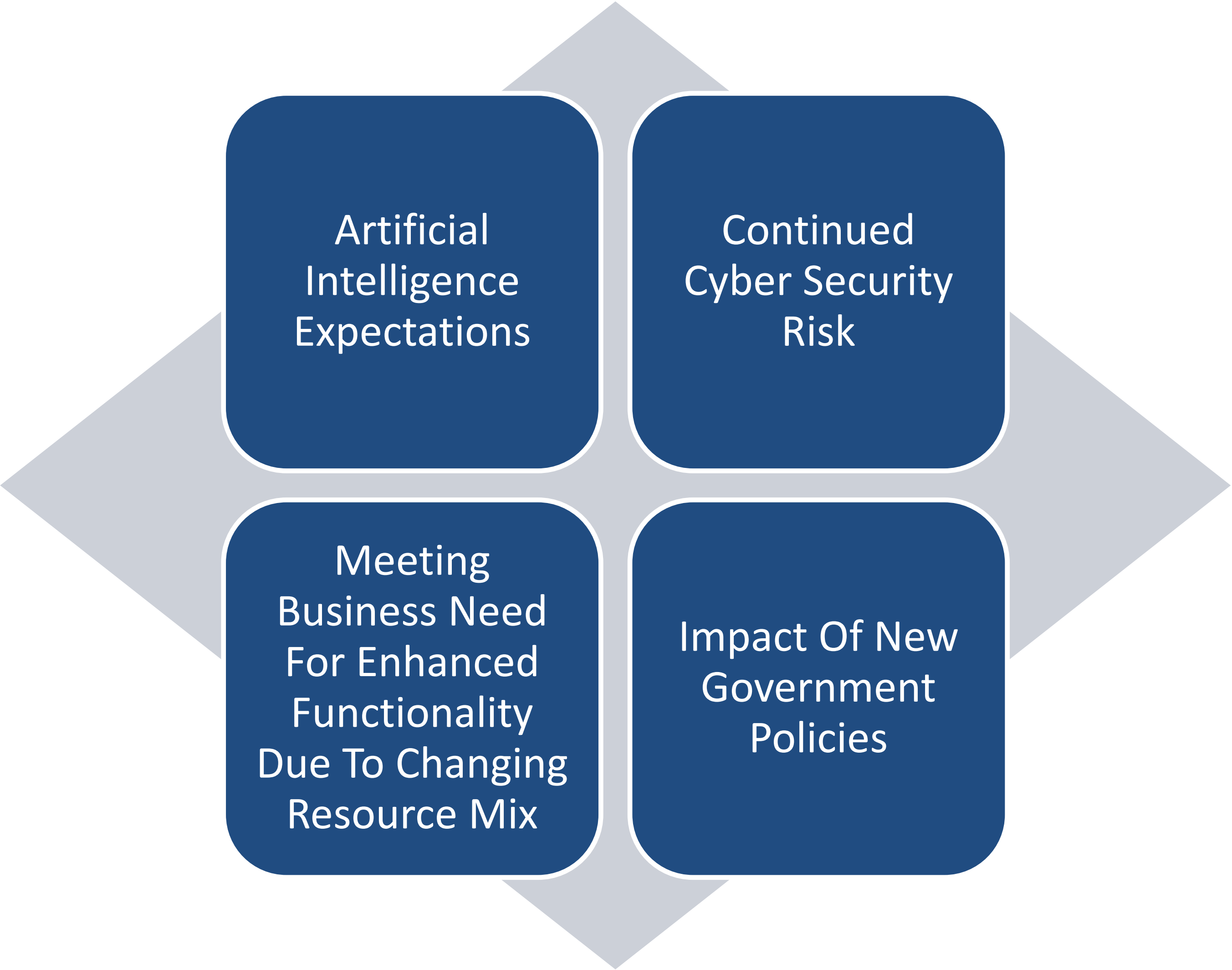
Data Science and Analytics

Data Modeling

Portfolio and Vendor Management

Business Relationship Management

Challenges



Artificial Intelligence Expectations

Continued Cyber Security Risk

Meeting Business Need For Enhanced Functionality Due To Changing Resource Mix

Impact Of New Government Policies

Value Proposition of 2026 IT Investments

The IT investments in 2026 “Bridge Year” are focused on enhancing foundational Cyber Security, Data Collection & Analytics, Stakeholder Outreach, and Infrastructure.

- Greater knowledge, awareness and response to cyber events
- Greater knowledge of Cold Weather events through improved data collection
- Heightened awareness of inverter-based resources through data collection
- Building IT infrastructure to support data analytics, modeling and reporting
- Stakeholder outreach and collaboration (better, more efficient outreach)
- Initial re-design, rebuild and simplification of foundation infrastructure

Questions and Answers

Agenda Item 3
Technology and Security Committee
Open Meeting
May 7, 2025

E-ISAC Operations

Action

Update

Summary

The E-ISAC remains vigilant, including heightened awareness throughout the start of 2025. It shared rapid electricity sector context about a variety of individual cyber and physical incidents, though there was no specific, credible, and imminent threat to the bulk power system. The E-ISAC continues its robust stakeholder engagement, focused on increasing the value of the products, programs and services provided to the members to enhance consumption and use of its information and analysis. Additionally, Michael Ball took the helm of the E-ISAC CEO and NERC Senior Vice President on April 14, 2025, from Manny Cancel; Cancel will remain as an advisor until the end of May 2025.

Bluma Sussman will report on recent strategic engagement efforts as well as the latest progress on the strategic implementation phase of the stakeholder experience effort, reviewing information consumption, event participation, stakeholder sentiment factors, and plans to operationalize this feedback in E-ISAC products and services.

Matt Duncan will summarize the threat landscape for the Committee with a focus on physical security incidents and ongoing Chinese and hacktivist cyber threats.

E-ISAC Strategic Engagement

The E-ISAC is a member-focused organization, and places great value not only in broadening the reach of this community to serve its diverse set of stakeholders, but also in developing deep and strong connections across the community, nurtured over time. Through prioritization of strategic outreach, the E-ISAC is investing long term in trusted relationships with members and partners to further information sharing and engagement in support of its mission to reduce risk to the North American electricity industry.

Over recent months, strategic engagement efforts include active participation with the following stakeholders and events:

- **Joint Action Agencies:** Relationship-building with leaders of municipal utilities at the Joint Action Conference.
- **NRECA's Tech Advantage:** Speaking with Rural Electric Co-Ops at about new options for GridEx.
- **DistribuTECH:** Engaging with utilities and vendors on securing emerging grid technologies.
- **FERC-NERC Joint Supply Chain Workshop:** Discussing ways to enhance vendor risk assessment and improve trust in procurement data.
- **ISC West's Security Industry Association Conference:** Speaking with technology integrators about reducing supply chain risk.
- **Industry Engagement Programs:** Hosting three IEPs for 32 members and partners, including five Vendor Affiliate Partner organizations.
- **Denmark-based SektorCERT:** Onboarding a new international partner, who maintains a network sensor program much like CRISP.

Canadian Partnerships

In a dynamic geopolitical environment, cross-border collaboration is essential. The E-ISAC's partnerships with Canadian government and trade associations demonstrate our ongoing commitment to strengthening and protecting the North American power grid. Recent engagements in Ottawa included meetings with Canadian government, trade associations, and asset owner operators. Highlights include:

- **Attending the Canadian Gas Association (CGA) Energy Security Summit** to discuss gas-electric coordination and cross-border issues.
- **Participating in the Energy Security Technical Advisory Committee (ESTAC) Q1 Meeting**.
- **Meeting with Canadian Government and trade partners** such as Electricity Canada, Natural Resources Canada (NRCAN), and the Canadian Centre for Cyber Security (CCCS).

Stakeholder/User Experience (UX): Content Optimization and Information Design

Since February, the E-ISAC has been working to enhance the products and services utilized by its members and partners, with support of stakeholder experience contractor Main Digital. The focus is on three guiding principles:

- Consistency
- Simplicity
- Easily digestible

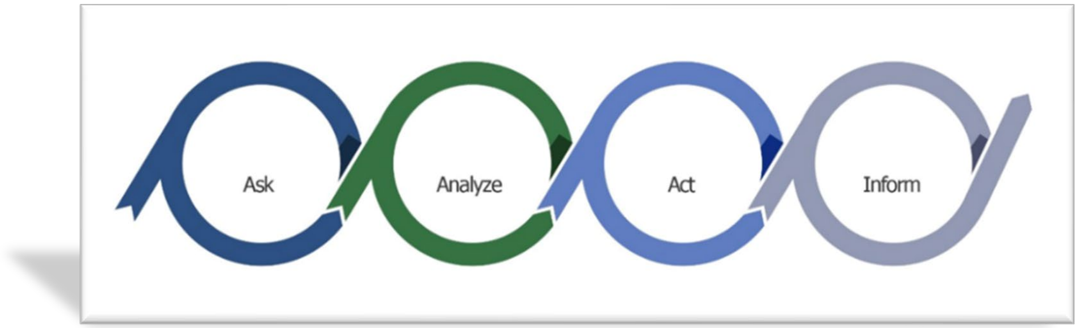
The goal is to ensure members can process critical information easily, knowing 'the what,' why, and what-to-do-next, immediately. These principles guide the design, titling, and structuring of information in E-ISAC products. The redesigned products aim to meet users where they are, whether they are executives at large utilities, analysts in control rooms, or general managers in small utilities.

Stakeholder Feedback Strategy

The E-ISAC has developed a centralized approach and process to ensure the E-ISAC strategically tracks and addresses stakeholder feedback. Enterprise-wide adoption of this process serves several business purposes:

- Informs enhancement of E-ISAC operations, product offerings, and process efficiencies
- Increases morale and validation (as feedback reinforces staff efforts, products, and programs)
- Drives continuous improvement of our members' experience

The E-ISAC Stakeholder Feedback Strategy is a four-step framework focused on continuous improvement. Actioning on this strategy will help identify member needs and pain points, guide future product development, and increase value members derive from E-ISAC content.



This approach involves the following four steps:

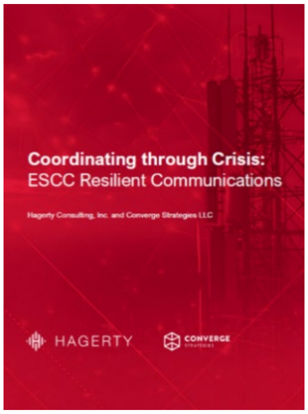
1. **Ask**: Gathering input and data directly from members via surveys, interviews, and rolling feedback.
2. **Analyze**: Using qualitative and quantitative methodologies to find patterns and insights.
3. **Act**: Sharing insights with stakeholders, creating a plan of action, exploring, creating, and testing solutions.
4. **Inform**: Sharing updates with the E-ISAC community, measuring the impact of new solutions, and focusing on continuous improvement.

UX Focus Groups

Four stakeholder focus groups were conducted to shape the redesign of the Portal homepage. Participants emphasized a desire for a cleaner homepage with easier access to high-use features. The new design reflects this feedback with simplified navigation and clear pathways to critical content and highly visible "calls to action."

Resilient Communications

Following recommendations from the GridEx VII Executive Tabletop exercise, the E-ISAC launched a resilient communications project in coordination with the ESCC. The project reviewed past communications efforts, analyzed existing processes, and provided recommendations for improving communications resilience. The PACE Communications methodology (Primary, Alternate, Contingency, Emergency) is strongly encouraged.



Coordinating through Crisis:
ESCC Resilient Communications

Hagerty Consulting, Inc. and Converge Strategies LLC

ESCC Directory

An outcome of the resilient communications project is the establishment of the ESCC Directory on the E-ISAC Portal. This directory is intended for ESCC executives and their plus ones, along with the Secretariat and other personnel in trade organizations with mutual aid roles. A copy of the directory will be emailed to those listed in the directory on a quarterly basis for offline use.

Threat Landscape

Across the threat landscape cyber and physical actors continue to target and attack the electricity industry with geopolitical and financial motivations. The 2025 U.S. Annual Threat Assessment highlighted a fresh perspective on threats to the U.S. Homeland and national interests, emphasizing the threat of terrorist and transnational criminal organizations. However, threats from Russia, China, Iran and North Korea remain significant threats

> … by attacking or threatening others in their regions, with both asymmetric and conventional hard power tactics…. They seek to challenge the United States and other countries through deliberate campaign to gain an advantage, while also trying to avoid direct war.[1]

The Canadian National Cyber Threat Assessment 2025-2026 provides a similar perspective describing cybercrime and geopolitics, stating:

> Canada is confronting an expanding and complex cyber threat landscape with a growing cast of malicious and unpredictable state and non-state cyber threat actors, from cybercriminals to hacktivists, that are targeting our critical infrastructure and endangering our national security.[2]

The North American electricity industry continues to face daily threats from both criminal and nation state actors from a cyber, physical and increasingly a hybrid perspective. Increased

[1] Tulsi Gabbard, Director of National Intelligence, March 2025, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

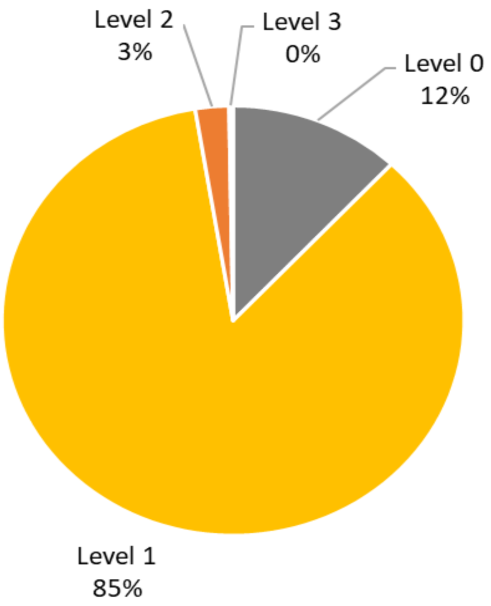
[2] Rajiv Gupta, Head, October 2024, Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

geopolitical and economic competition and rhetoric will likely further complicate the threat landscape and industry supply chains.

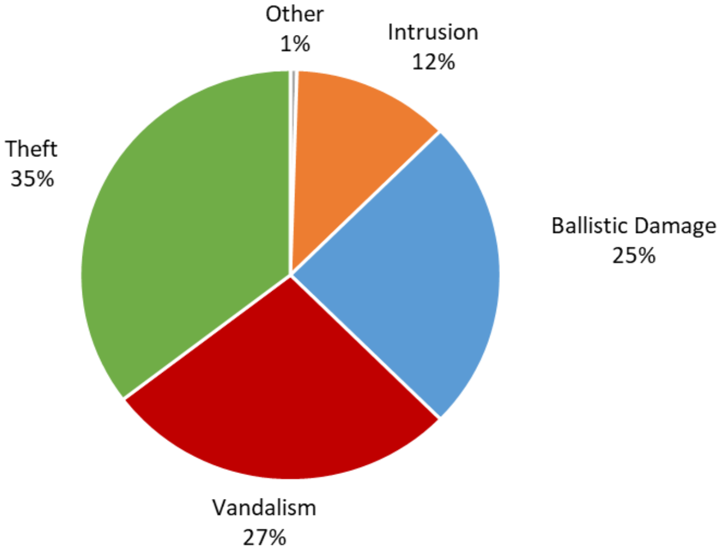
Physical Security - Grid Impacting Incidents (2023-2024)

The E-ISAC recently released its annual grid impacting incidents report to members and partners, highlighting the frequency of physical security incidents causing operational impacts to the grid remains consistent, averaging less than three percent per year since 2020.

The report analyzes incidents shared with the E-ISAC in 2024 compared to historical data. As threat actors diversify their targets and tactics, this analysis helps utilities make informed risk-based decisions to assist in protecting their critical assets. Statistical coverage of the industry has also increased and improved, with sharing in 2024 increasing 45% as additional utilities voluntarily share physical security incident data with the E-ISAC for analysis.



Severity Level Breakdown 2020-2024
Level 0 – *Non-criminal, general activity*
Level 1 – *Criminal no outages*
Level 2 – *Criminal, 9,999 cust/1-19MW out*
Level 3 *– Criminal, 10k+/20MW+ out*



Grid Impacting Incidents by Incident Type 2023-2024

Vandalism, theft (primarily copper), ballistic damage, and intrusion (including tampering) were the most frequently reported incident types resulting in operational impacts. The most common vandalism tactic that resulted in operational impacts involved cut wires, 36% of which targeted fiber-optic cabling a concerning finding consistent with other critical infrastructure sectors. Impacts from cut wires ranged from customer outages to generation unavailability across a variety of electric assets, including third-party infrastructure. The E-ISAC assesses that 37% of grid impacting incidents in 2024 were likely sabotage, which is matched by 69% of online threats assessed by E-ISAC aspiring to sabotage against the grid.

While there is no one-size-fits-all approach for implementing protective measures against these threats, the report highlights physical resources available to industry that can help members develop appropriate protective measures, including a physical security guide and Vulnerability of Integrated Security Analysis (VISA) workshops, as well as sharing information with the E-ISAC.

Cyber Security – Actors and Tradecraft

The People’s Republic of China (PRC) cyber actors, such as Volt-, Salt-, and Silk-Typhoon, remain active and persistent in targeting critical infrastructure networks in the U.S. and Canada, including electricity. Cyber activity by the PRC remains focused on reconnaissance and prepositioning in networks.

The E-ISAC continues to track a variety of hacktivist and ransomware groups targeting the electricity industry through its open-source intelligence collection program. Given geopolitical tensions there is a renewed focus by “hacktivists,” or hackers with a particular motivational cause, on particularly U.S. critical infrastructure given ongoing economic competition as well support for the state of Israel. It is unclear the geopolitical allegiances of these groups as they often have conflicting ideologies but nevertheless require industry defenders to spend time and resources countering their tradecraft, primarily rudimentary hacking, website defacement, and distributed denial of service (DDoS) attacks.

Regardless of whether actors are geopolitical, criminal, or hacktivists, the E-ISAC observed continued targeting of network edge devices as actors of all stripes seek to gain opportunistic access to utility information and operational technology systems. While obtaining legitimate credentials via social engineering, phishing, or insider threat are often ideal, the availability of botnet obfuscation networks, significant computing power, and artificial intelligence-based tools have increased the threat from repetitive or iterative approaches making “educated guesses” on passwords or overwhelming protections at scale. While none of these attacks have resulted in customer outages, reporting of these techniques has increased in 2025.

Cyber Tradecraft Observed by E-ISAC

- Targeting of **network edge devices**
- **Brute Force and SYN Flood** attempts against networks and VPNs
- **Botnets used to obfuscate** origin of attacks and reconnaissance
- **Distributed Denial of Service (DDoS)** attacks seen against the sector websites
- Unverified claims on social media/dark web of **data leaks or ransomware**

The E-ISAC continues to work with trusted partners in the U.S. and Canadian governments, as well as the telecommunications, gas, and other critical infrastructure sectors, sharing best practices for detecting living off the land activity and anomalous activity. The Cybersecurity Risk Information Sharing Program (CRISP) is a cornerstone of that effort for the electricity industry and will continue to evolve in technology and efficiency as it looks to expand coverage to cope with these threats.

A DIVISION OF NERC

E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Stakeholder Experience

Bluma Sussman, Vice President, Stakeholder Engagement
Technology and Security Committee Meeting
May 7, 2025

Engagement in Action

- **Strengthen** supply chain risk management
- **Enhance** grid resilience and security of small and medium size utilities
- **Promote** secure adoption of emerging T&D technologies and build relationships with utilities and vendors

NRECA America's Electric Cooperatives

DISTRIBUTECH

AMERICAN PUBLIC POWER ASSOCIATION

SIA SECURITY INDUSTRY ASSOCIATION

DEPARTMENT OF ENERGY FEDERAL ENERGY REGULATORY COMMISSION

Canadian Partnerships

- **Reinforce cross-border partnerships** in a sensitive geopolitical climate
- **Enhance coordination** on gas-electric interdependencies
- **Align on shared approaches** to energy security and emergency preparedness
- **Emphasize commitment** to protect the North America bulk power system

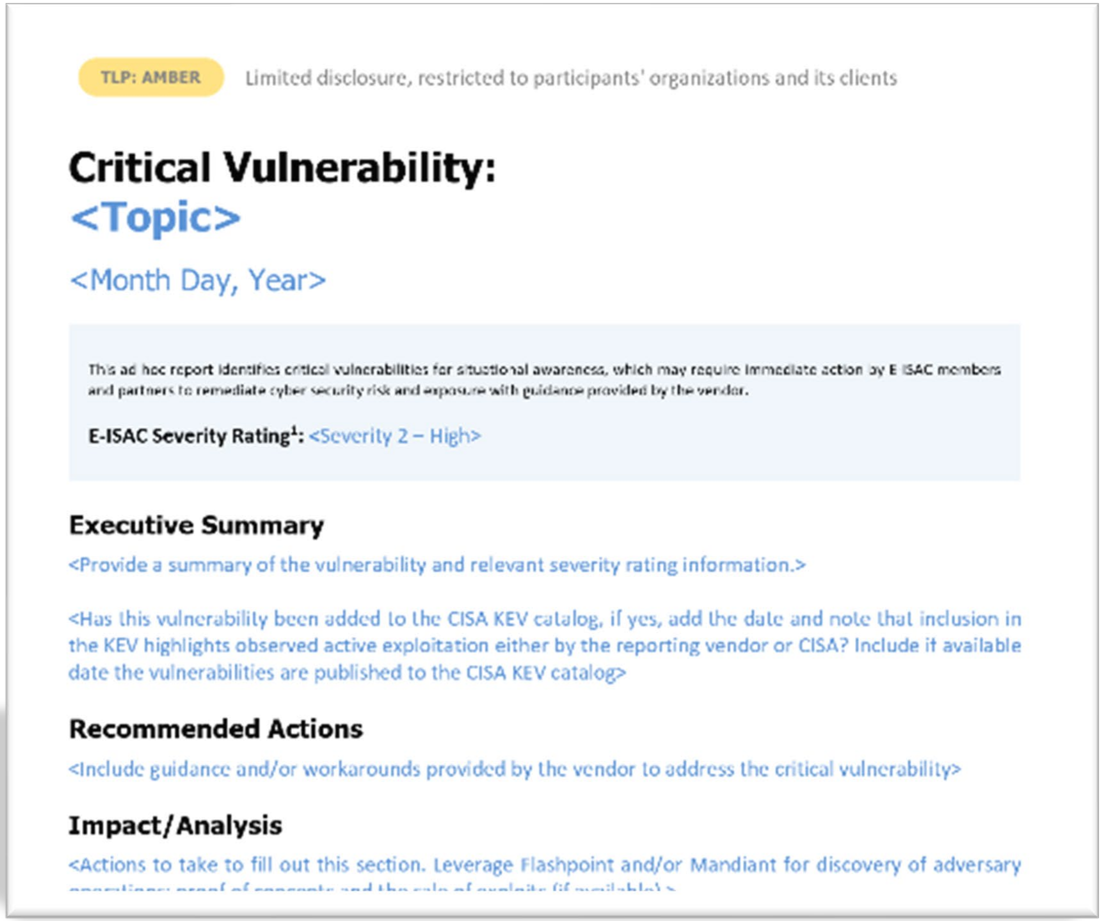
Content Optimization and Information Design

Portal Content Guiding Principles

CONSISTENCY

SIMPLICITY

EASILY DIGESTABLE



TLP: AMBER Limited disclosure, restricted to participants' organizations and its clients

Critical Vulnerability: <Topic>

<Month Day, Year>

This ad hoc report identifies critical vulnerabilities for situational awareness, which may require immediate action by E-ISAC members and partners to remediate cyber security risk and exposure with guidance provided by the vendor.

E-ISAC Severity Rating[1]: <Severity 2 – High>

Executive Summary

<Provide a summary of the vulnerability and relevant severity rating information.>

<Has this vulnerability been added to the CISA KEV catalog, if yes, add the date and note that inclusion in the KEV highlights observed active exploitation either by the reporting vendor or CISA? Include it available date the vulnerabilities are published to the CISA KEV catalog>

Recommended Actions

<Include guidance and/or workarounds provided by the vendor to address the critical vulnerability>

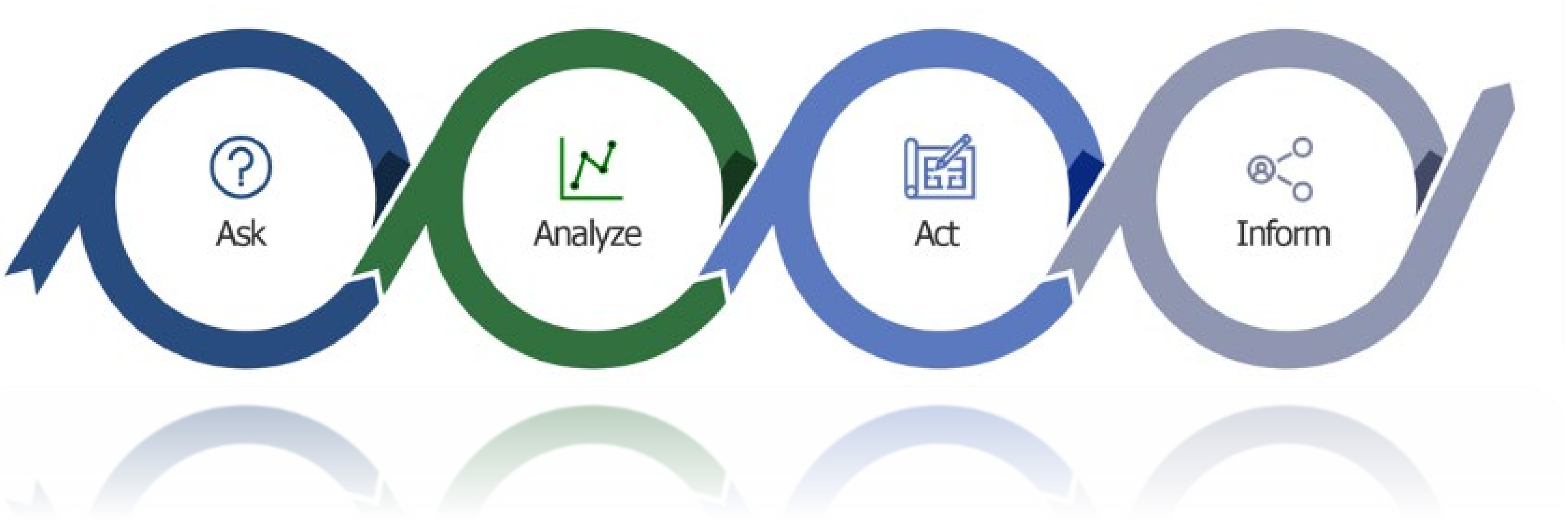
Impact/Analysis

<Actions to take to fill out this section. Leverage Flashpoint and/or Mandiant for discovery of adversary operations; proof of concepts and the sale of exploits (if available).>

Stakeholder Feedback Strategy

Feedback Strategy Channels

- ✓ Surveys
- ✓ Cases and Emails
- ✓ Focus Groups



UX Focus Groups

Portal Homepage Redesign

- Facilitated multiple focus groups
- Gathered direct input from members to improve Portal usability
- Centered on Solutions that meet stakeholder needs

Key Takeaways

- ✓ Highly visible “Call to Action”
- ✓ Enhance main menu navigation
- ✓ Enable increased data on CRISP reports

Resilient Communications

Coordinating through Crisis:
ESCC Resilient Communications

Hagerty Consulting, Inc. and Converge Strategies LLC

PACE = Primary, Alternate, Contingency, Emergency

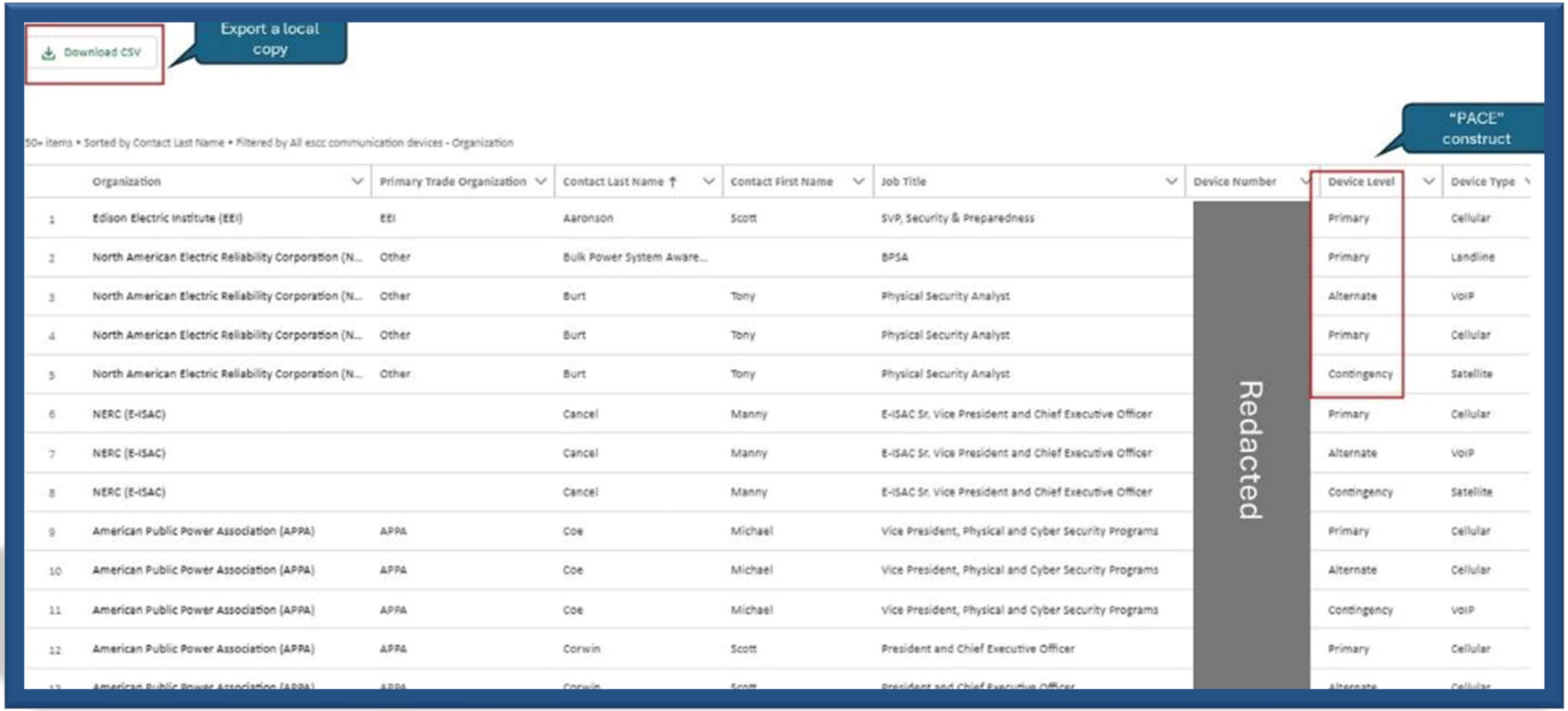
Report Key Outcomes

- Establish ESCC Directory on E-ISAC Portal
- Incorporate PACE planning into ESCC Playbook
- Institute ESCC Playbook training
- Integrate ESCC Playbook into GridEx Executive Tabletop

Next Steps

- Distribute Report
- Industry to operationalize findings

ESCC Directory



50+ items • Sorted by Contact Last Name • Filtered by All escc communication devices - Organization

	Organization	Primary Trade Organization	Contact Last Name ↑	Contact First Name	Job Title	Device Number	Device Level	Device Type
1	Edison Electric Institute (EEI)	EEI	Aaronson	Scott	SVP, Security & Preparedness	Redacted	Primary	Cellular
2	North American Electric Reliability Corporation (N...	Other	Bulk Power System Aware...		BPSA		Primary	Landline
3	North American Electric Reliability Corporation (N...	Other	Burt	Tony	Physical Security Analyst		Alternate	VoIP
4	North American Electric Reliability Corporation (N...	Other	Burt	Tony	Physical Security Analyst		Primary	Cellular
5	North American Electric Reliability Corporation (N...	Other	Burt	Tony	Physical Security Analyst		Contingency	Satellite
6	NERC (E-ISAC)		Cancel	Manny	E-ISAC Sr. Vice President and Chief Executive Officer		Primary	Cellular
7	NERC (E-ISAC)		Cancel	Manny	E-ISAC Sr. Vice President and Chief Executive Officer		Alternate	VoIP
8	NERC (E-ISAC)		Cancel	Manny	E-ISAC Sr. Vice President and Chief Executive Officer		Contingency	Satellite
9	American Public Power Association (APPA)	APPA	Coe	Michael	Vice President, Physical and Cyber Security Programs		Primary	Cellular
10	American Public Power Association (APPA)	APPA	Coe	Michael	Vice President, Physical and Cyber Security Programs		Alternate	Cellular
11	American Public Power Association (APPA)	APPA	Coe	Michael	Vice President, Physical and Cyber Security Programs		Contingency	VoIP
12	American Public Power Association (APPA)	APPA	Corwin	Scott	President and Chief Executive Officer		Primary	Cellular
13	American Public Power Association (APPA)	APPA	Corwin	Scott	President and Chief Executive Officer		Alternate	Cellular

Questions and Answers

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

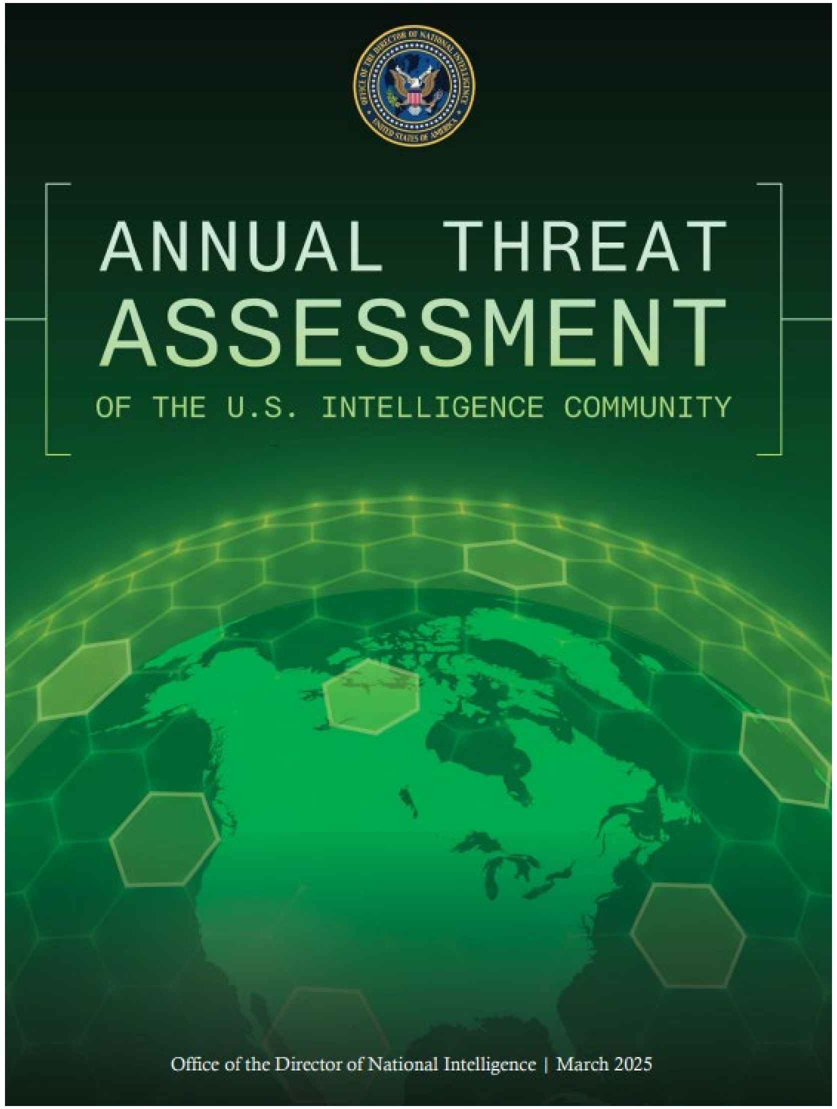
E-ISAC Security Operations and Intelligence Update

Matt Duncan, Vice President, Security Operations and Intelligence
Technology and Security Committee Meeting
May 7, 2025

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

U.S. and Canadian Threat Assessments



ANNUAL THREAT ASSESSMENT

OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence | March 2025

CANADIAN CENTRE FOR CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT

2025
2026

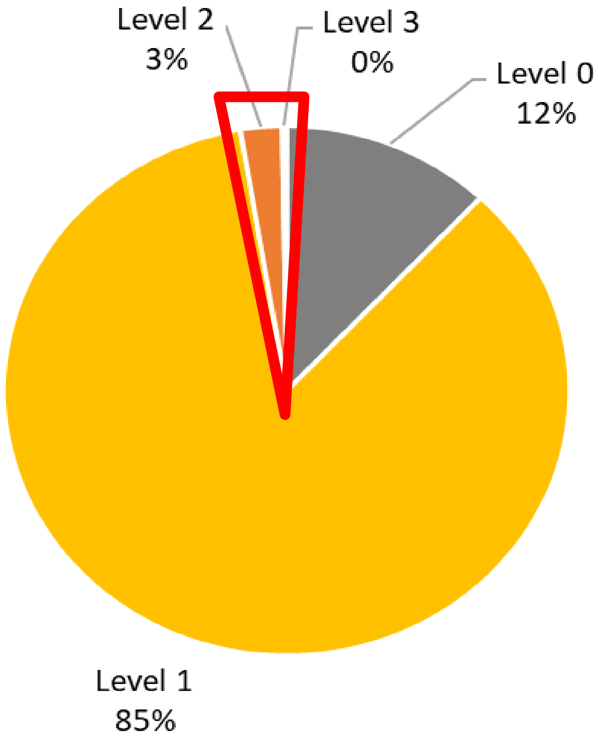
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada
Canadian Centre for Cyber Security
Centre canadien pour la cybersécurité

Canada

Grid Impacting Incidents (2023-2024)

- Level of grid-impacting incidents less than 3% since 2020
- Economic factors and online rhetoric
- 37% of incidents indicate sabotage
- Vandalism, theft, ballistic damage, and intrusion most common share types
- Damaged wires, including fiber optic cables, most common vandalism type

Physical Security Incidents Causing Outages



Severity Level Breakdown 2020-2024

Level 0 – *Non-criminal, general activity*
Level 1 – *Criminal, activity with no outages*
Level 2 – *Criminal, 9,999 customers/1-19MW outages*
Level 3 *– Criminal, 10k+ customers /20MW+ outages*

Cyber Security – Actors and Tradecraft

People’s Republic of China (PRC) Cyber

- Continued activity by Volt, Salt, Silk Typhoons

“Hacktivists”

- Claimed activity by a variety of groups of varying motives

Tradecraft

- Continued targeting and attacks against networking devices
- Brute force and flooding attempts against networks and VPN
- Botnets used to obfuscate origin of attacks

Questions and Answers