NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Technology and Security Committee Meeting

August 13, 2025 | 9:00 – 10:00 a.m. Mountain

In-Person
The Westin Calgary Downtown
320 4th Avenue SW
Calgary, Alberta, Canada T2P 2S6

Conference Room: Britannia/Belaire/Mayfair Ballroom – Conference Level

Virtual Attendees
Webcast Link: Join Meeting
Webcast Password: Day1Aug25ATT (32912843 from phones)
Audio Only: 1-415-655-0002 US | 1-416-915-8942 Canada | Access Code: 2304 717 8300

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. May 7, 2025 Open Meeting*
2. **E-ISAC Operations* — Update**
3. **ERO Enterprise Artificial Intelligence (AI)* — Update**
4. **Other Matters and Adjournment**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Technology and Security Committee
Open Meeting

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

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

Call to Order

Ms. Jane Allen, 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 7, 2025, at approximately 11:00 a.m. Eastern, and a quorum was declared present.

Present at the meeting were:

Committee Members	**Board Members**
Jane Allen, Chair	Kenneth W. DeFontes, Jr.
Larry Irving	George S. Hawkins
Susan Kelly	Robin E. Manning
Jim Piro	James B. Robb, President and Chief Executive Officer
Suzanne Keenan, *ex officio*	Kristine Schmidt
	Colleen Sidford

NERC Staff

Michael Ball, Senior Vice President and Chief Executive Officer of the E-ISAC
Tina Buzzard, Director, Board Operations and Corporate Governance
Manny Cancel, Advisor to the Chief Executive Officer of the E-ISAC
Todd Carter, Vice President Business Technology
Matthew Duncan, Vice President, E-ISAC Security Operations and Intelligence
Howard Gugel, Senior Vice President, Regulatory Oversight
Kelly Hanson, Senior Vice President and Chief Operating Officer
Mark Lauby, Senior Vice President and Chief Engineer
Sonia Rocha, Senior Vice President, General Counsel, and Corporate Secretary
Camilo Serna, Senior Vice President, Strategy and External Engagement
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

Ms. Allen welcomed participants to the meeting and reviewed the agenda. She welcomed Mr. Carter and Mr. Ball and requested Mr. Robb to provide a more fulsome introduction, which Mr. Robb provided. Ms. Allen also acknowledged that this was Mr. Cancel's last TSC meeting and she thanked him for his tremendous efforts through his years with NERC.

Minutes

Upon motion duly made and seconded, the Committee approved the minutes of the February 12, 2025, open meeting as presented at the meeting.

ERO Enterprise Business Technology Strategy

Ms. Allen welcomed Mr. Carter, NERC's new Vice President of Business Technology. Mr. Carter provided an update on the implementation of the ERO Enterprise Business Technology Strategic Plan. His update focused on critical 2026 business technology investments. The Committee discussed the update to nerc.com and use of artificial intelligence for bulk power system operations.

E-ISAC Operations

Ms. Sussman reported on the E-ISAC's 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. The Committee discussed the development of the ESCC Directory and testing it in GridEx.

Mr. Duncan summarized the threat landscape for the Committee with a focus on physical security incidents and ongoing Chinese and hacktivist cyber threats. The Committee discussed links between cyber and physical security attacks, increased incident reporting, the recent outages in Spain and Portugal, and common threat landscapes for other sectors.

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
August 13, 2025

E-ISAC Operations

Action
Update

Summary
The E-ISAC remains vigilant, maintaining heightened awareness to the current geopolitical climate and encouraging members to adopt and sustain a Shields Up posture to strengthen their online security posture. Iranian, Chinese, Russian, North Korean and other threat actors remain active on the cyber espionage front. Criminal organizations, hacktivists, and extremists continue to demonstrate the ability and desire to impact critical infrastructure across North America.
Bluma Sussman will report on recent strategic engagement efforts as well as progress updates on the stakeholder experience effort inclusive of content optimization and E-ISAC Portal User Experience upgrades. She will also brief the Board of Trustees (Board) on upcoming E-ISAC events this Fall.

Matt Duncan will summarize the threat landscape and E-ISAC's response and actions to date, highlighting physical security incidents and cyber threats for the Board in this open session. Additionally, Matt will summarize the E-ISAC's operational engagement with Canada, emphasizing the importance of maintaining strong cross-border relationships in today's geopolitical climate.

Strategic Engagement
The E-ISAC is committed to its members and partners, placing a high value on longstanding relationships and community connections. Strategic outreach across a diverse stakeholder base enables us to foster trust and enhance information sharing. Our engagements continue to prioritize meaningful participation that advances key Work Plan Priorities and our broader strategic plan.

Recent strategic engagement efforts include:

- **Solar/Renewables:** Fostering new relationships with renewable energy organizations at Solarplaza and ACP's Annual Meeting, Cleanpower, to compliment the NERC IBR Registration Initiative.
- **Public Power & Joint Action Agencies:** Relationship-building with leaders of municipal utilities at the APPA National Conference.
- **Small & Medium Co-ops:** Engaging with cooperatives at NRECA Co-op Cyber Tech and discussing products specifically designed for small and medium utilities.
- **Canadian Partnerships:** Participating in a series of meetings with Canadian government, trade associations, and asset owner operators to reinforce our commitment to cross-border collaboration.
- **Supply Chain Risk Management:** Welcoming industry leaders, like Microsoft and Siemens, as the newest members of our Vendor Affiliate Program (VAP). These strategic partnerships enhance the program's mission to deliver valuable insights, technical expertise, and threat intelligence to our members – strengthening supply chain risk management.

GridEx VIII

Hosted every two years by the E-ISAC, GridEx gives E-ISAC member and partner organizations a forum to test their emergency response capabilities to recover from major disruptions from coordinated cyber and physical security attacks.

In addition to leading planning and coordination efforts for a full-scale exercise with over 15,000 players, the E-ISAC has added two new options for participation in GridEx VIII. New play options offer easier, more accessible participation for small teams and newcomers, while expanding opportunities for organizations of all sizes and capabilities.

GridSecCon

Registration for GridSecCon 2025 opened in early June and registration to date is well ahead compared to previous years. The conference agenda features a full day of hands-on training and over 30 breakout sessions covering a wide range of energy sector trends, challenges, and best practices; such as insider threat, distributed energy risks, artificial intelligence, OT cyber security, and cross-border reliability coordination.

Content Optimization & Design

In Q2, the E-ISAC implemented recommendations from the discovery phase of a broader stakeholder experience initiative in the following areas: Content Optimization, Information Design, and Stakeholder Feedback. These refinements increase the reach and impact of information by the E-ISAC. This work also resulted in the development of a comprehensive Digital Delivery Strategy which integrates personas and audience segmentation to enhance engagement, improve outreach effectiveness, and drive measurable results for distributing content through the E-ISAC's digital channels.

Feedback Strategy

The E-ISAC also formalized a comprehensive Feedback Collection and Analysis Strategy; promoting continuous improvement across E-ISAC products and services to codify processes around the management, analysis, actioning and sharing of stakeholder feedback.

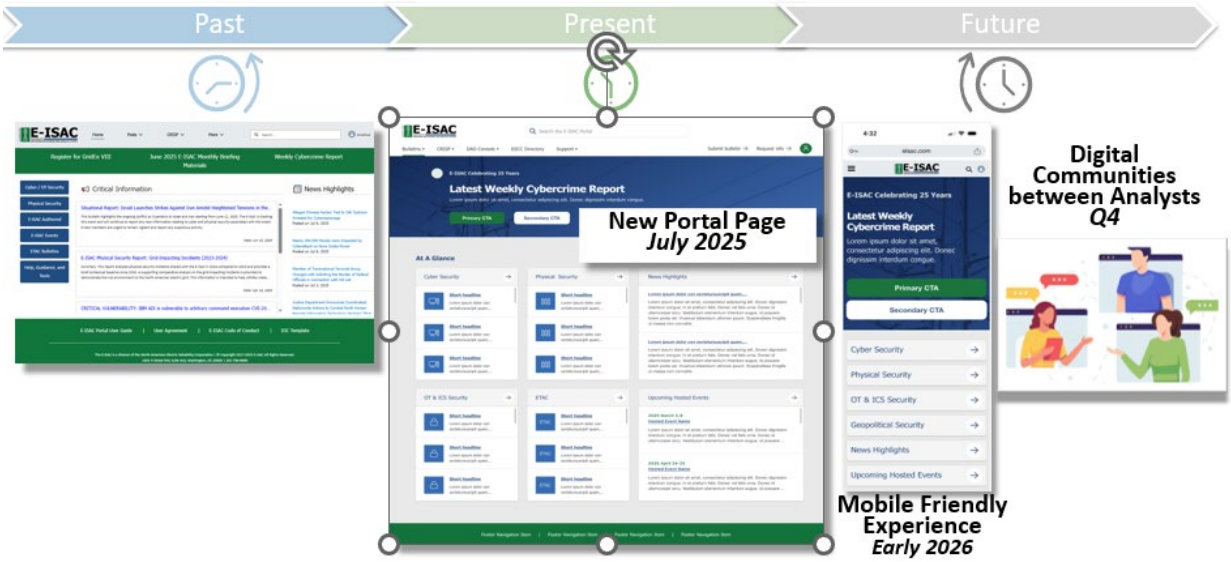
Additionally, the E-ISAC will take immediate action on this strategy via the delivery of a bi-annual Stakeholder Feedback Survey for all E-ISAC members and partners this October. As in previous years, the E-ISAC will collaborate with J.D. Power to develop, deliver and analyze the survey results, and anticipate updating the Board on the results of the Survey in February 2026.

User Experience

User Experience improvements to the E-ISAC Portal continue in an incremental manner. Improvements were informed by multiple member focus groups held in 2024 and early 2025. Over the last six months the interface for Designated Approving Officials (DAOs) was revised to include better navigation, filtering, and pop-up call-to-action banners for annual reviews while existing features were enhanced in terms of usability. CRISP reports and data files were incorporated into the Portal enabling the retirement of Pacific Northwest National Laboratory's legacy CASA application. A new Energy Threat Analysis Center (ETAC) specific page was also added, allowing interested parties to quickly find bulletins authored by that team.

In July, a revised home page and main navigation menu will be released promoting ease of use to rapidly find important industry reports or bulletins. In the fall, bulletin pages and other subpages will be revised to reflect the new navigation, layout, and aesthetic standards. Bulletins and bulletin email notifications will also be enhanced to include more useful, well-organized

information on the web page and in the email body versus in file attachments, thus making it easier for members to quickly discern relevance.



2025 Open-Source Intelligence Monitoring and Direct Shares

The E-ISAC is tracking threat activity targeting both cyber and physical aspects of the electricity sector as well as other critical infrastructure sectors. People's Republic of China (PRC) state-sponsored actors such as Salt Typhoon and Volt Typhoon – continue activity against critical infrastructure. China remains a persistent espionage threat to critical infrastructure and the electricity industry, and the E-ISAC is working with industry and government to develop real-world scenarios defensive scenarios to exercise with during GridEx in November.

Ransomware operators, cybercrime forum users, and politically motivated hacktivist groups also continue to launch attacks against energy sector entities worldwide. Domestic Violent Extremists (DVEs) are actively using online image boards to promote violence against North American electricity infrastructure and are exploiting political divisions to spread ideological messaging, share tactical guidance, and encourage sabotage against the grid.

The E-ISAC is tracking the ongoing Israel-Iran conflict, which the United States entered on June 22 with bombings against nuclear enrichment sites in Iran. Specifically, the E-ISAC continues to monitor open-source intelligence and CRISP data for any cyber activity against North American electrical infrastructure for possible retaliation of Iranian cyber actors targeting vulnerable U.S. networks and entities of interest. The E-ISAC encountered increases in activity by pro-Iran hacktivist groups claiming to carry out attacks, primarily DDoS attacks, against U.S. and Israeli organizations across numerous sectors. Though DDoS activity continues to be the routine technique for hacktivist activity in general, the E-ISAC continues to observe some hacktivists claiming to breach industrial control systems (ICS) in specifically targeted victim countries – most typical are pro-Russia operations targeting European sectors.

The E-ISAC monitors ransomware groups and cybercrime forums, among other OSINT and dark web platforms, to track claimed attacks targeting energy sector entities – including utilities, oil and gas companies, and vendors. These forums also enable the sale of stolen data and unauthorized access, which threat actors use to launch more damaging follow-on attacks. The E-ISAC continues to enhance and refine its direct share processes to reduce vulnerability severity across the sector and expand coverage of social media and dark web spaces. By strengthening its ability to identify and share timely insights on geopolitical activity, hacktivist campaigns, and credential-based threats, the E-ISAC aims to provide members with actionable intelligence to better examine and mitigate risks.

Ransomware and Cybercrime Update:

- 263 total incident claims observed in first six months of 2025
- Only four involved targeting of OT/SCADA systems
- 1,982 direct shares sent to members and partners from January 1 – June 30, 2025
- Direct shares increased by 79% from this same time period last year (1,109 to 1,982) due to operational efficiencies in E-ISAC capabilities
- Canadian E-ISAC members and partner organizations received 250 of these shares accounting

Canadian Partnerships

In a dynamic geopolitical environment, cross-border operational 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. In 2025, the E-ISAC made several key cross-border engagements, strengthening its commitment to support Canadian electricity asset owners and operators and government partners.

This year, the E-ISAC has increased engagement with counterparts from the following Canadian organizations:

- **Canadian Centre for Cyber Security** facilitating two-way information-sharing and collaboration on cybersecurity challenges as well as participation in GeekWeek, a forum for cyber security professional to collaborate on solutions to vital issues facing industry
- **Canadian Gas Association** to support training and development efforts and promotion of E-ISAC products to broaden Canadian stakeholder awareness
- **Electricity Canada** coordinating on cross-border security priorities and emerging threats
- **Canadian Association of Members of Public Utility Tribunals** sharing insights on evolving cyber threat landscape and protective strategies on panel at annual conference
- **NRCAN** through partnership through the Energy and Utilities Sector Network enhancing cross-border situational awareness and participating in Energy Cyber CONOPS Command Post Exercise

Other Canadian partners include Public Safety Canada, the Independent Electricity System Operator, and the Royal Canadian Mounted Police.

The E-ISAC and the Canadian Security Establishment (CSE) re-signed an information sharing agreement on March 10, 2025. This allows for two-way sharing of information with the Canadian Centre for Cyber Security (CCCS), the cybersecurity branch of CSE, and the E-ISAC. Both the E-ISAC and CCCS participate in recurring monthly planning discussions supporting E-ISAC events and specific cyber event releases. The E-ISAC recently participated in GeekWeek, which is an annual unclassified workshop hosted by CCCS bringing together key players in the cyber security field to work together on generating solutions to vital problems facing industry. During GeekWeek, the E-ISAC contributed to ICS honeypots and scanning for malicious infrastructure teams and labs.

The E-ISAC is an active participant in the EnerSec CCCS program providing a cyber threat briefing at monthly meetings, Electricity Canada's Security and Infrastructure Protection Committee (SIPC) quarterly meetings and participated on a panel at the annual CAMPUT conference for Canada's energy and utility regulators regarding the current threat landscape as well as strategies

necessary to protect against cyber threats. Lastly, the E-ISAC attended the CGA Energy Security Summit in March 2025 and is working with CGA to provide recommendations on an analyst training element for next year's summit.

The E-ISAC participated in the Energy Command Exercise with Natural Resources Canada (NRCan) Energy Cyber Concept of Operations (ConOps) Command Post Exercise (CPX). This was a functional exercise that confirmed identified lines of communication within the Energy ConOps when cyber threat information thresholds and triggers have been met. The collaboration between the E-ISAC and NRCan through the Energy and Utilities Sector Network (EUSN) strengthens cross-border information sharing and situational awareness critical to the security of the North American grid. NRCan promotes E-ISAC initiatives like GridSecCon and shares selected E-ISAC bulletins, when authorized, to raise awareness among Canadian stakeholders broadening the reach of vital intelligence products.

The E-ISAC's partnerships with Canadian government and industry organizations are essential to strengthening the resilience and security of the North American bulk power system. Cyber and physical threats do not recognize national borders–coordinated, cross-border collaboration enhances situational awareness, improves threat detection and response, and ensures timely information sharing during critical events.

E-ISAC Stakeholder Experience

Bluma Sussman, Vice President, Stakeholder Engagement
Technology and Security Committee Open Meeting
August 13, 2025

Strategic Engagement

Engagement in Action

Strong relationships, effective collaboration, and meaningful engagement are crucial to meeting our mission.

- **Advancing** cross-border partnerships
- **Enhancing** resilience and security of small and medium utilities
- **Fostering** new relationships with renewable energy organizations
- **Strengthening** supply chain risk management

Strategic Engagement

GridSecCon 2025

- SOLD OUT in 2024
- 15% increase in 2025 registration
- Topics range from grid security and resilience to cross-border collaboration

GridEx VIII

- New distributed play offerings for smaller planning teams
- 25% increase in registration from GridEx VII
- Executive Tabletop Exercise on Nov 20, 2025

Stakeholder Experience

Focus on Content

- More **consistent**
- **Simpler** and cleaner
- Easier to **digest**

36
Project Activities Completed

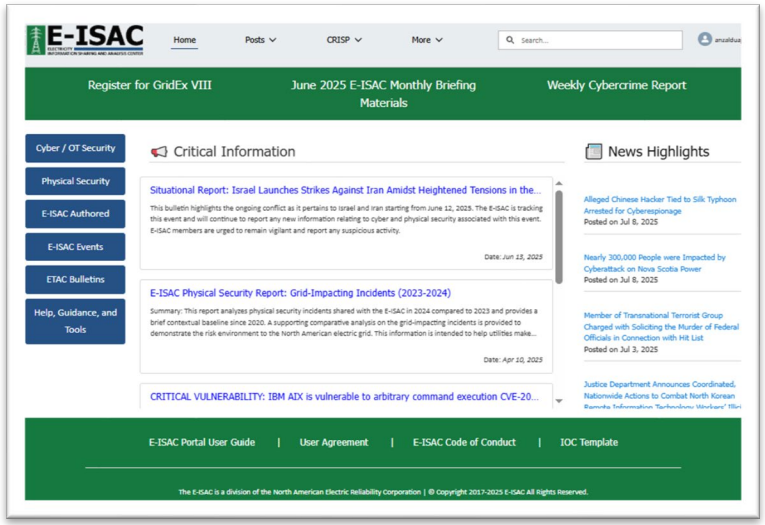
14
Content Model Components Defined

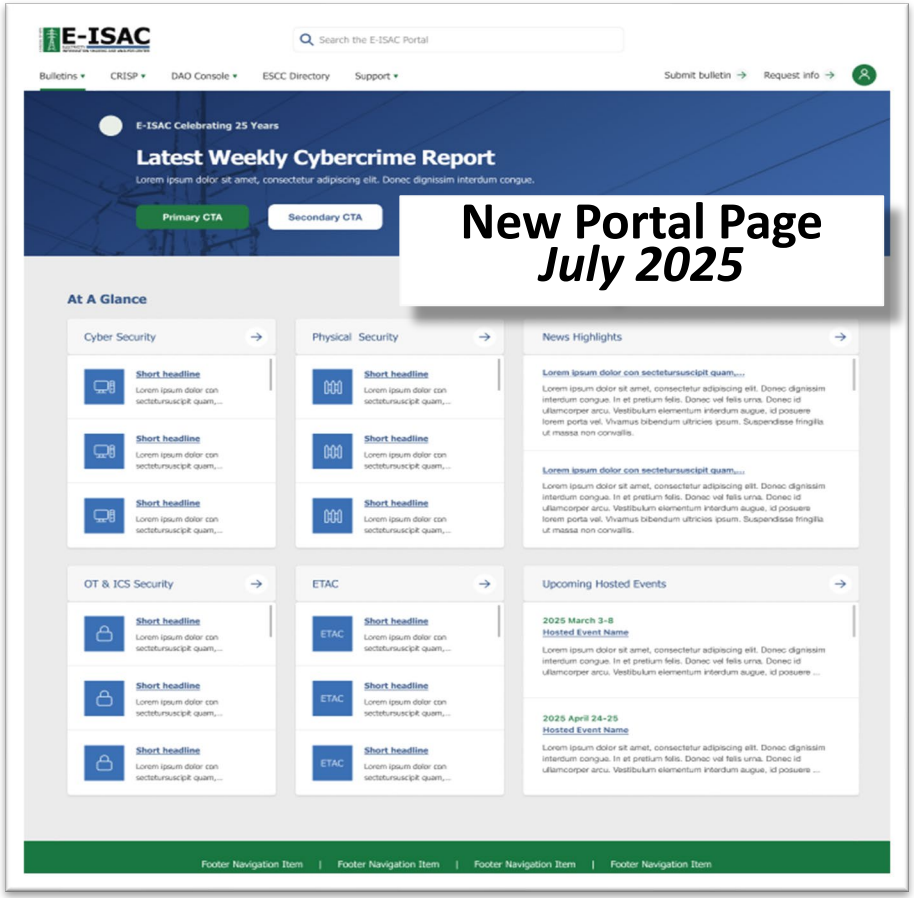
33
Products Audited

16+
Internal Stakeholders Contributing

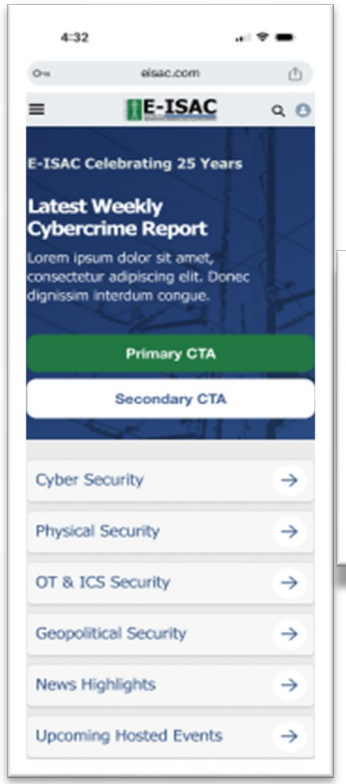
09
Design Assets Produced

Past | Present | Future



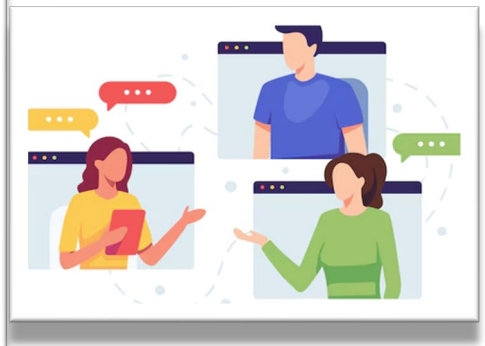


New Portal Page
July 2025



Mobile Friendly Experience
Early 2026

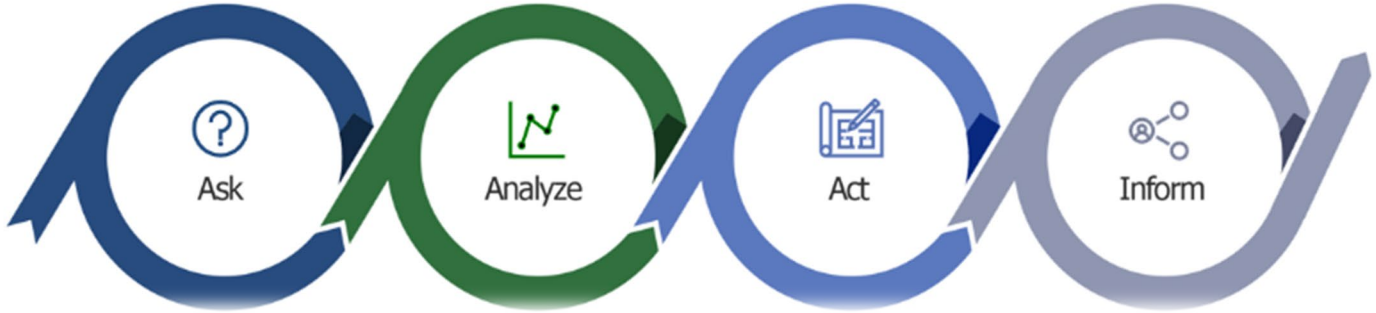
Digital Communities between Analysts
Q4



Stakeholder Experience

Feedback Collection and Analysis

- Adaptability & relevance
- Continuous improvement
- Stakeholder advocacy



E-ISAC Stakeholder Feedback Survey

- **Release timeline:** October 2025

CUSTOMER SATISFACTION
J.D. POWER AND ASSOCIATES
SINCE 1968

J.D. POWER

Questions and Answers

E-ISAC Security Operations & Intelligence

Matthew Duncan, Vice President, Security Operations & Intelligence
Technology and Security Committee Open Meeting
August 13, 2025

Security Operations and Intelligence

Current Threat Landscape

- **China-linked actors remain a threat**
- **Proactive threat intelligence** resulted in **1,982** direct shares to member and partner organizations in 2025
  - **79% increase** compared to 2024
  - **43% increase** in shares to utility members
  - **13% increase** in shares to Canadian members and partners
- **Geopolitical events motivate and inspire** threat actors
  - **Pro-Iran hacktivist groups and DDoS attacks**
  - **CRISP enhanced monitoring following attacks on Iran**
- **Ransomware and Cybercrime Forums** in 2025
  - **263 global energy sector claims tracked**

Security Operations and Intelligence

Canadian Collaboration

In 2025, E-ISAC conducted key **cross-border engagements**, demonstrating its commitment to Canada. The enhanced **information sharing** strengthens critical infrastructure security for all North America.

- Regular briefings, working groups, tabletop exercises
- Panel participation on threat landscape with energy and utility regulators
- Agreements for two-way sharing of confidential information
- Collaboration between CRISP, Blue Flame, and Lighthouse programs
- Participation at CCCS GeekWeek Unclassified Workshop
- Additional outreach to UK, Australia and New Zealand

Questions and Answers

ERO Enterprise Artificial Intelligence (AI)

Action
Update

Summary
AI is an emerging technology that offers significant promise to many industries. AI has dominated media headlines across most of the modern world, capturing the spirit of innovation that spans beyond traditional methods of human machine interfaces, interactions, and uses. The ERO Enterprise has embarked on a journey to identify and pilot how it can apply AI across NERC and the Regional Entities in a way that upholds the ERO Enterprise's responsibility to safeguard confidential and restricted registered entity data while balancing the ERO Enterprise's ability to leverage and achieve the benefits and promises of this emerging technology.

Todd Carter, NERC's Vice President Business Technology, Howard Gugel, NERC's Senior Vice President, Regulatory Oversight, and Joseph Younger, Texas Reliability Entity, Inc., Vice President and Chief Operating Officer will provide the Technology and Security Committee with an update on the status of AI within the ERO Enterprise. They will discuss the guiding principles underlying the ERO Enterprise's AI strategy and review current and future uses of AI. As this update is intended as the first of many, the presentation will begin with a series of interactive questions for the audience, which will give us a sense of the audience's role, their understanding of AI, and their understanding of ERO Enterprises' approach to AI. This data will help shape future AI discussion topics.

Why AI Matters
AI matters because it fundamentally changes how we solve problems, make decisions, and interact with the world. Understanding AI helps individuals to adapt, compete, and stay informed in a rapidly evolving world. AI is attracting significant investment that is expected to grow as demand skyrockets and value is realized.

Current NERC AI Activities

Generative AI Use Case Ideation
In April 2024, NERC engaged a vendor to conduct a Generative AI Use Case Ideation and Prioritization Analysis. The vendor conducted interviews across the ERO Enterprise and identified 65 Gen AI use cases that would likely improve productivity, enhance decision-making, and reduce consistent pain points identified across the ERO Enterprise. Of the 65 total use cases, 36 were considered in-scope and applicable to business process areas across the ERO Enterprise.

Here are a few examples of the illustrative use cases identified:

- **Standards Development Comment and Feedback Summarization:** Develop an AI solution to ingest and summarize feedback, develop trends, recommend changes to standards, and draft responses to comments.

- **General Workflow Optimization Using Chatbots:** Deploy chatbots and other utilities for tasks, such as sending reminders for AI requests and optimizing workflows.
- **Develop NERC Alert Response Summaries:** Summarize and/or generate reports on NERC Alert Responses.
- **Root Cause Analysis:** Analyze key data sources and pinpoint root causes behind situations. Use this to proactively identify entities with similar configurations where the same situation may occur.
- **Commonly Violated Standards:** Review trends of commonly violated standards and use this to create education materials.

Overview of AI Pilots

In August 2024, NERC management chose to pilot the chatbot and standards summarization use cases. Reliability First (RF) also began a Microsoft Co-Pilot initiative in January 2025. The following is a brief overview of those pilots.

ERO AI Chatbot Pilot

A significant amount of public information exists related to the Compliance Monitoring and Enforcement Program (CMEP), but it is not always clear where to find the most current information, or where relevant support materials, guidance documents, and the development record are located. Creating an AI Chatbot well-versed in these materials for ERO Enterprise staff use could significantly reduce the time required to quickly find and apply the knowledge required to perform CMEP tasks. The first iteration of this new tool will be internal use only for the ERO Enterprise.

Current Status: NERC is taking advantage of one of Microsoft's partner programs using Unify Cloud's AI Factory. The AI Factory provides several use case "accelerators," in which key technology and implementation patterns have been established for use ahead of time based on best practices. One of those accelerators is an "AI Chatbot for Company Laws and Policies," which will assist customers in developing a chatbot that can "automate responses to legal and policy-related queries, assisting employees in understanding corporate regulation, and ensuring easy access to legal documents." NERC is working to engage Applied Information Sciences (AIS) to use this accelerator to meet NERC requirements as described above. This pilot is expected to begin in the third quarter of 2025 and deliver results in the fourth quarter of 2025.

AI Standards Summarization Pilot

NERC began its AI journey with a policy exception to allow one person in Standards Development to explore the use of AI to assist in the summarization of submitted comments, which is an existing part of the Standards Development Process currently performed by staff and drafting team members. Because all comments and responses are part of the public record, and because drafting teams are required to review and respond to all comments, the risk of using AI for this task was low. Initial experimentation using Open AI's Chat GPT product found significant potential for time savings. The purpose of this project is to build on this initial effort by identifying and implementing an AI solution that can assist the entire Standards team.

Current Status: NERC has acquired a Chat GPT Enterprise license and has developed a custom GPT (Generative Pre-trained Transformer) with instructions specific to the Standards process. This tool is currently being used in parallel with human efforts to verify and validate performance

of the GPT. Training is in development for the Standards staff with the goal of expanding usage once users are trained and NERC Single Sign-On has been established within Chat GPT. This Pilot is expected to be completed in the third quarter of 2025.

Microsoft CoPilot Pilot
ReliabilityFirst (RF) began a limited test phase of Microsoft 365 (M365) CoPilot (consisting of IT and Security) in January 2025 to understand the technology. RF learned that M365 CoPilot, once enabled, grants the same file visibility rights to the user, emphasizing the importance of role-based access controls and recurring access authorization audits. We have since been able to learn and test protective controls, enable and centralize the detective controls, and craft training that communicates the procedural controls.

Current Status: RF has created a multi-pronged security strategy for the safe and reliable use of M365 CoPilot, consisting of a series of technical controls, interactive user training, logging, monitoring, and alerting. RF has implemented access authorization audits, role-based access controls, and training, and then enabled M365 CoPilot for ~35 users, with plans to reach 50 by August 2025. RF has avoided work teams whose work is primarily focused on core CMEP functions.

ERO Enterprise Governance Approach

The ERO Enterprise is taking a conservative approach toward AI, ensuring industry data is safe and secure, and any AI initiative is performed responsibly. The ERO Enterprise will leverage the NIST Artificial Intelligence Risk Management Framework to define the governance and management model for AI across the ERO. The **NIST AI Risk Management Framework (AI RMF)** is a comprehensive guide designed to address the risks associated with AI systems. It aims to promote the responsible development and deployment of AI technologies while minimizing potential harms and maximizing benefits. The following is a discussion of AI risks and the NIST AI RMF's approach to managing them.

AI systems pose unique risks that differ from traditional software systems due to their complexity, adaptability, and socio-technical nature. These risks include:

- **Bias and Fairness**: AI systems can amplify harmful biases present in training data, leading to discrimination or inequitable outcomes. Managing systemic, computational, and human-cognitive biases is critical.
- **Privacy Concerns**: AI systems often rely on large datasets, which may include sensitive or personally identifiable information (PII). Risks include data leakage, unauthorized use, and de-anonymization.
- **Security Vulnerabilities**: AI systems are susceptible to adversarial attacks, data poisoning, and model extraction, which can compromise their integrity and reliability.
- **Explainability and Transparency**: Many AI systems lack interpretability, making it difficult for users to understand their decisions or outputs. This can erode trust and accountability.
- **Environmental Impact**: Training and operating AI models, especially large-scale ones, consume significant computational resources, contributing to carbon emissions.
- **Safety and Reliability**: AI systems must operate safely under defined conditions without endangering human life, property, or the environment. Failures in safety-critical applications can have severe consequences.

The NIST AI RMF provides a structured approach to managing these risks through four core functions:

1. **Govern**: Establish a culture of risk management by implementing policies, processes, and accountability mechanisms. This includes aligning AI practices with organizational values, legal requirements, and ethical standards.
2. **Map**: Identify and document the context, intended use, and potential impacts of AI systems. This involves understanding the socio-technical environment and assessing risks at different lifecycle stages.
3. **Measure**: Develop and apply metrics to evaluate AI risks, including trustworthiness characteristics such as fairness, privacy, and security. Regular testing and monitoring are essential to ensure system performance aligns with expectations.
4. **Manage**: Prioritize and address identified risks through mitigation **strategies**, continuous monitoring, and improvement. This includes planning for incident response and system decommissioning when necessary.

To enhance trustworthiness, AI systems should exhibit the following attributes:

- **Valid and Reliable**: Ensure accuracy and robustness across diverse conditions.
- **Safe and Secure**: Protect against failures, adversarial attacks, and unauthorized access.
- **Accountable and Transparent**: Provide clear documentation and enable traceability of decisions.
- **Explainable and Interpretable**: Offer insights into how decisions are made and their implications.
- **Privacy-Enhanced**: Safeguard user data and uphold privacy norms.
- **Fair**: Mitigate harmful biases and promote equitable outcomes.

The NIST AI RMF is designed to be flexible and adaptable across sectors and use cases. Organizations can use it to:

- Conduct risk assessments and prioritize mitigation efforts.
- Align AI practices with regulatory requirements and societal values.
- Foster interdisciplinary collaboration and stakeholder engagement.
- Develop tailored profiles for specific applications, such as hiring or healthcare.

By adopting the NIST AI RMF, organizations can navigate the complexities of AI risk management, ensuring that AI technologies are developed and deployed responsibly, ethically, and sustainably.

Management will continue to provide an array of meaningful and insightful AI-related topics at NERC Board meetings to educate and demonstrate what the ERO Enterprise is doing and how it is maintaining its responsibility to be trustworthy stewards of confidential and restricted data across the ERO Enterprise while benefiting from safe and secure use of AI tools to improve our effectiveness.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Artificial Intelligence (AI) Update

Todd Carter, Vice President, Business Technology
Howard Gugel, Senior Vice President, Regulatory Oversight
Joseph Younger, Vice President & Chief Operating Officer, Texas Reliability Entity Inc.

Technology and Security Committee Open Meeting
August 13, 2025

Today's Discussion Topics

- Introductions
- Today's Agenda
  - Why AI matters
  - How are we using AI today in the ERO Enterprise
  - What near-term AI activities do we see
  - How will we govern and manage AI
  - Our commitment to you
- Word Cloud - Final Question

Why AI Matters ?

AI is attracting significant private investment. Generative AI alone attracted >$34B in 2024.

78% of global organizations reported using AI in 2024. Up from 55% in 2023

AI requires a vastly different approach to adoption than other new technologies; like any powerful tool, its impact depends on how we choose to use it

The ERO Enterprise will take a conservative approach toward AI, ensuring industry data is safe and secure and any AI initiative is performed responsibly.

Current AI Activities Within the ERO Enterprise

- Partnered with a vendor to build a set of AI use cases that will allow us to increase our understanding of what is needed to securely deploy, govern and manage AI technology throughout the ERO Enterprise.

- Currently piloting Generative AI, limiting our reach to publicly available data, to gain efficiencies and improved productivity in several areas:
  - Standards Summarization
  - AI Chatbot
  - MS Pilot (limited reach)

- We will continue to pursue opportunities to leverage AI for efficiencies and productivity improvements in a conservative way.

Near-Term AI Opportunities

- Buildout foundational AI infrastructure and controls that can securely support AI initiatives.
- Develop training and change management programs to educate staff and key stakeholders.
- Continue the ongoing AI pilots.
- Evaluate other opportunities to securely use AI to transform and to gain efficiencies across the ERO Enterprise.

Our AI Governance Approach

- To guide our AI Governance approach, we are using the NIST AI Risk Management Framework (NIST AI RMF) v1.0 and input from internal and external groups:
  - Legal (LG)
  - IT Security Group (ITSG)
  - Analytics Center of Excellence (ACE)
  - Operations Leadership Team (OLT)

MIDWEST RELIABILITY ORGANIZATION
NPCC, Inc.
RELIABILITY FIRST
SERC
TEXAS RE
Ensuring electric reliability for Texans
WECC

ERO Enterprise AI Principles Development Framework

Key concepts of the NIST AI RMF that each organization are required to meet:

- Conduct a risk assessment of all AI systems.
- Maintain an inventory of all AI systems along with the data classification those systems handle.
- Develop AI training for personnel.
- Maintain appropriate human oversight over AI System outputs.
- Evaluate, periodically, AI Systems for safety and security risks.

We will also leverage existing IT security principles, data classification, and handling protocols.

Our Commitment to You

We, along with most organizations, are adapting to the benefits of leveraging Artificial Intelligence, which is emerging as we speak.

- We will continue to provide updates to the Technology and Security Committee.
- We do not intend to take undue risks with AI.
- We understand our responsibilities when it comes to the proper protection of stakeholder data in our possession.
- Adopt a posture of being a “fast follower” when it comes to AI. We think this is appropriate given the conservative nature of the ERO Enterprise and the exciting prospects we see with a disciplined and well-thought-out AI adoption strategy.
- As the AI marketplace, technology toolset, and industry continue to evolve, our commitment is unwavering in managing your data in a secure, reliable, and confidential manner.

NERC is the steward of sensitive registered entity data and will always manage this data in a secure, reliable and confidential manner.

Questions and Answers