

# Agenda 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

Conference Room: Grand Ballroom (5<sup>th</sup> Floor)

## Virtual Attendees

Webcast Link: [Join Meeting](#)

Webcast Password: FEB2025BRDTECHA (33220253 when dialing from a phone)

Audio Only: +1-415-655-0002 US Toll | +1-416-915-8942 Canada Toll | Access code: 2314 546 6229

## Committee Members

Jane Allen, Chair  
Larry Irving  
Suzanne Keenan  
Susan Kelly  
Robin E. Manning  
Jim Piro  
Kenneth W. DeFontes, Jr., *ex-officio*

## Introduction and Chair's Remarks

## [NERC Antitrust Compliance Guidelines](#)

## Agenda Items

1. **Minutes\* — Approve**
  - a. August 14, 2024 Open Meeting
2. **ERO Enterprise Business Technology Strategic Plan\*— Update**
3. **ERO Enterprise Stakeholder Engagement\*— Update**
4. **E-ISAC Operations\*— Update**
  - a. Threat Landscape
  - b. E-ISAC Customer Experience
5. **Other Matters and Adjournment**

\*Background materials included.

## Draft Minutes Technology and Security Committee Open Meeting

August 14, 2024 | 8:30-9:45 a.m. Pacific

In-Person  
Hyatt Regency Vancouver  
655 Burrard St.  
Vancouver, BC V6C 2R7, Canada

### 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 August 14, 2024, at approximately 8:30 a.m. Pacific, and a quorum was declared present.

Present at the meeting were:

### Committee Members

Jane Allen, Chair  
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, Director Intelligence  
Howard Gugel, Vice President, Regulatory Oversight  
Kelly Hanson, Senior Vice President and Chief Operating Officer  
Fritz Hirst, Vice President, Government Affairs  
Soo Jin Kim, Vice President, Engineering and Standards  
Mark Lauby, Senior Vice President and Chief Engineer  
Justin Lofquist, Director, Enterprise Application Architecture  
Sonia Rocha, Senior Vice President, General Counsel, and Corporate Secretary  
Liz Saunders, Vice President, People and Culture  
Camilo Serna, Senior Vice President, Strategy and External Engagement  
Andy Sharp, Vice President and Chief Financial Officer  
Bluma Sussman, Director, Membership  
Angus Willis, Director Information Technology Infrastructure and Support

**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.

**Minutes**

Upon motion duly made and seconded, the Committee approved the minutes of the May 8, 2024, open meeting as presented at the meeting.

**Technology and Security Committee Mandate**

Chair Allen noted that the NERC Legal Department has reviewed the current Committee mandate with the Committee Chair and members and is not recommending any revisions at this time.

**E-ISAC Operations**

Mr. Duncan summarized the recent CrowdStrike software issue that impacted numerous cloud services and shared lessons learned from the incident. Mr. Willis relayed there was no impact to the ERO Enterprise from the incident. Mr. Duncan following with a summary of the cyber and physical security threat landscape facing the electricity industry and discussed E-ISAC activities to address these threats and vulnerabilities.

Ms. Sussman reviewed the E-ISAC's recent efforts to further improve the stakeholder experience and offer meaningful opportunities for E-ISAC members and partners to learn, network, and engage.

**NERC Enterprise Analytics**

Mr. Lofquist discussed NERC's Business Technology group's efforts to advance and support analytics capability across the ERO Enterprise, including for the areas of Energy Assessments, Bulk Power System Awareness, Power Systems Analysis and Transfer capability. He reported on successful initiatives thus far and future areas of opportunity. The Committee led a discussion of these efforts, addressing security, data availability, and implementation considerations.

**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 Strategic Plan**

### **Action**

Update

### **Background**

Management will provide an update on the implementation of the ERO Enterprise Business Technology Strategic Plan on the investments completed in 2024 and planned for 2025, which is tracking according to plan.

The following investments were implemented in 2024 to continue to improve operational efficiencies for back end office processes as well as enhance security protocols, and implemented applications to enable the business:

- Sustainability
  - New Financial System – implemented a solution that would improve finance and accounting operational system.
  - Additional Features for HR System – implemented the compensation and recruitment functionality.
  - Enhancements for IT Case Management – improved ticket process and provide reporting metrics.
- Agility
  - Align Enhancements – the team deployed two releases to enhance the Align solution, which were for Attestations, Mitigations and Periodic Data Submittal.
  - Enhanced Collaboration Tools – implemented tools that would improve internal and external communications.
  - Registration Enhancements – implemented changes to the CORES solution.
- Security
  - Data Loss Prevention – implemented additional security protocols around data protection.
  - Identity Access Management – implemented a solution to manage automated employee and contractor provisioning and deprovisioning.
  - Application Security – increased security testing of ERO Enterprise applications to ensure compatibility with security best practices.

- Energy
  - Analysis System for Wind and Solar – two applications were implemented to allow entities (generator owners) to provide solar generation and wind turbine data per NERC Section 1600.
  - Reliability Coordinator Information System – NERC’s Rules of Procedure stipulate the use of RCIS as the primary method of communication between Reliability Coordinators (RC), Balancing Authorities (BA), and Transmission Operators (TO).
  - Reliability Assessment Database Design

The following technology investments are planned for 2025:

- Sustainability
  - New Public Website – implement a website to improve customer interaction with NERC.
  - Stakeholder Collaboration Platform – implemented the compensation and recruitment functionality.
  - Application Platform Upgrades – upgrade the platform to continue maintaining critical business applications.
- Agility
  - Align Enhancements – continue to enhance the Align solution to improve stakeholder experience.
  - Operator Certification Database – identify a vendor to replace the System Operator Certification Database to manage user experience.
  - Design for Enterprise Analytics – identify the requirements and design model for data provided by entities that are utilized by NERC departments.
- Security
  - Additional Cloud Security Capabilities – implement cloud security controls for threat prevention and detection around additional cloud infrastructure.
  - Desktop Operating System – ensure NERC user equipment is secure and up to date.
  - Enhanced Endpoint Protection and Monitoring – implementation of an enhanced cyber security strategy to monitor and protect devices from cyber threats.
- Energy
  - Registration for Inverter-Based Resources – IBRs will contribute to a resilient and sustainable future energy landscape. Register the IBR owners and operators that are connected to the bulk power system.
  - Cold Weather Data Collection – provide a generator collection area for worksheet submissions.
  - Reliability Assessment Database – implement an automated data solution to collect, validate, and store reliability assessment data.

**NERC**

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# ERO Enterprise Business Technology Strategic Plan

Stan Hoptroff, VP, Business Technology  
LaCreacia Smith, Director, Project Management Office  
Technology and Security Committee Open Meeting  
February 12, 2025

RELIABILITY | RESILIENCE | SECURITY



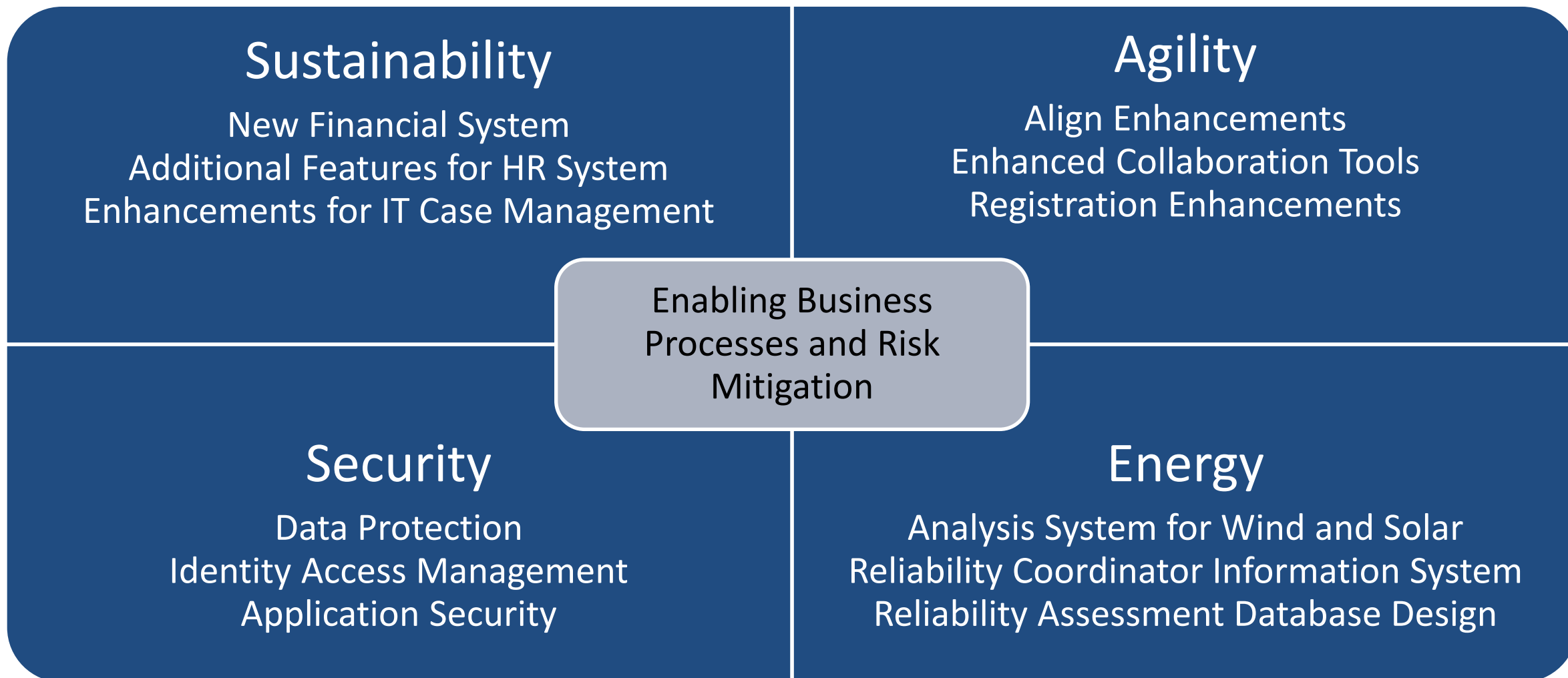
2024 Business Technology Journey

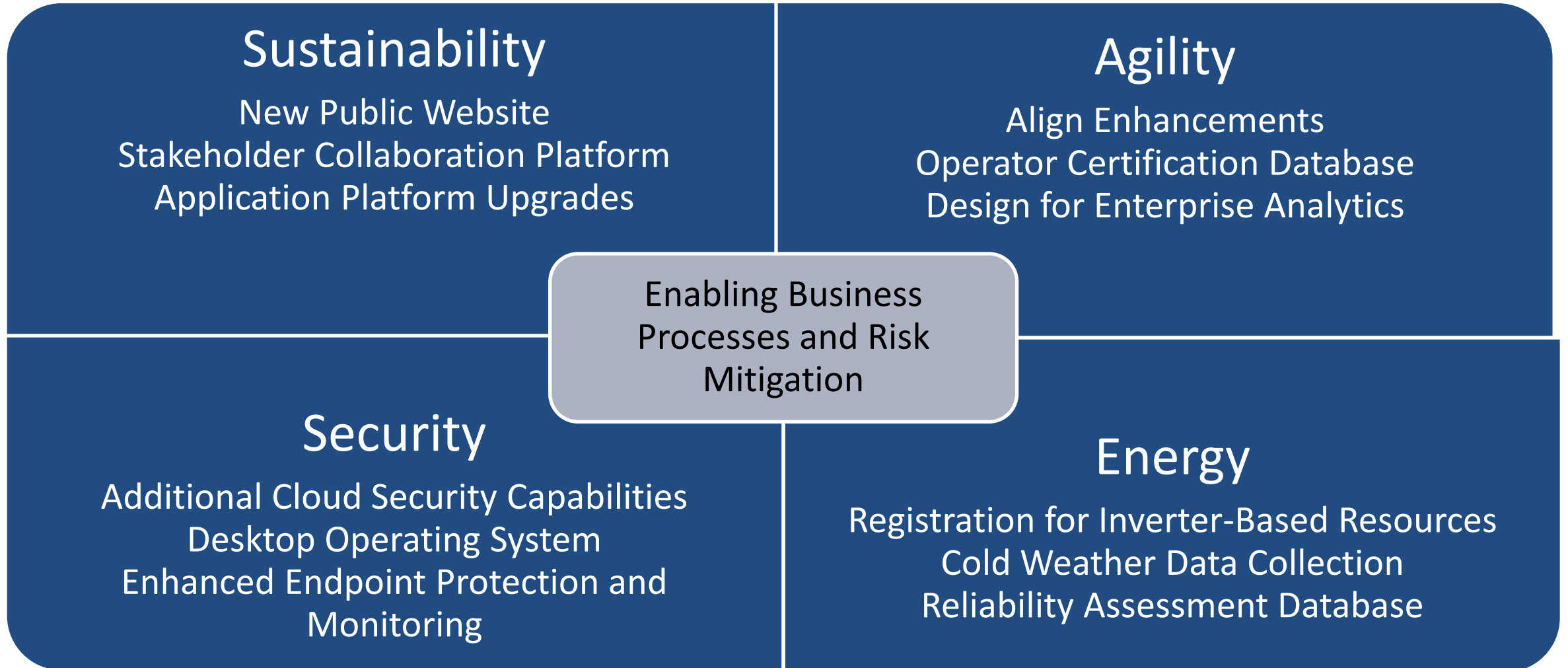


2025 Business Technology – Final Year of Three-Year Plan











# Questions and Answers

## **ERO Enterprise Stakeholder Engagement**

### **Action**

Update

### **Background**

Management will provide an overview of the results of the 2024 ERO Enterprise Business Technology client survey. The purpose of the survey is to assess customer satisfaction with the Business Technology department and identify areas for continued improvement.

The survey was conducted between December 2, 2024, and January 15, 2025, respondents to the survey included:

- Registered Entities (51%)
- Regional Entities (12%)
- NERC Staff (12%)
- Trade Organizations (10%)
- Stakeholders (6%)
- Vendors (5%)
- Regulators (4%)

There was a 17% increase in survey participation over 2023.

### **Summary**

The results of the survey show that satisfaction with NERC's Business Technology improved from 2023 (in both customer support and Business Technology overall). The survey highlighted the following key areas for continued improvement:

- Making it easier to report issues
- Better notification to customers on status of reported issues
- Speed of issue resolution
- Ensuring responses resolve the reported issue

The NERC logo consists of the letters "NERC" in a bold, black, sans-serif font. A horizontal blue bar is positioned directly beneath the text.

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

# 2024 NERC Business Technology Survey Results

Stan Hoptroff, Vice President, Business Technology  
Technology and Security Committee  
February 12, 2025

RELIABILITY | RESILIENCE | SECURITY

## Who

- Stakeholder Community

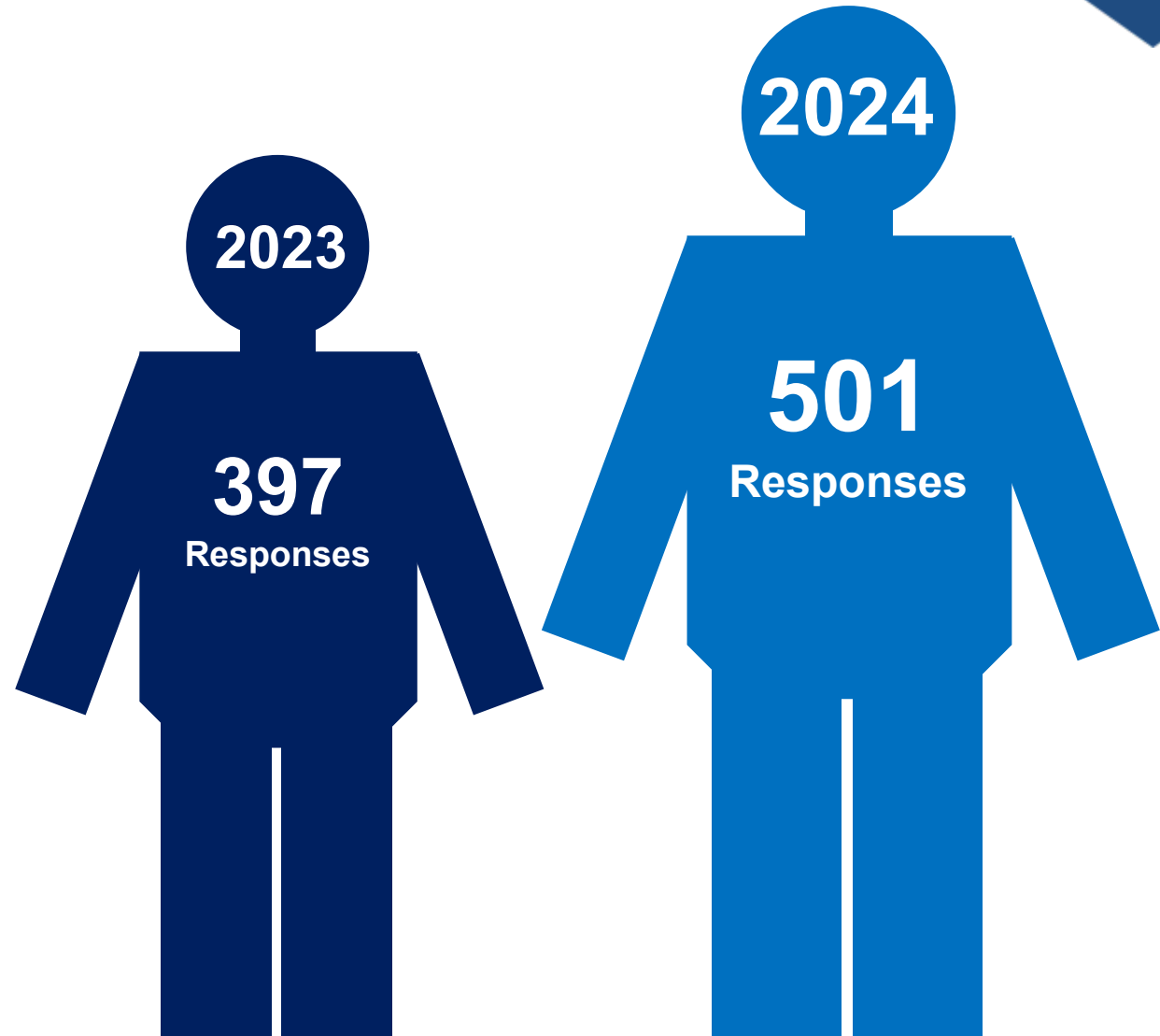
## When

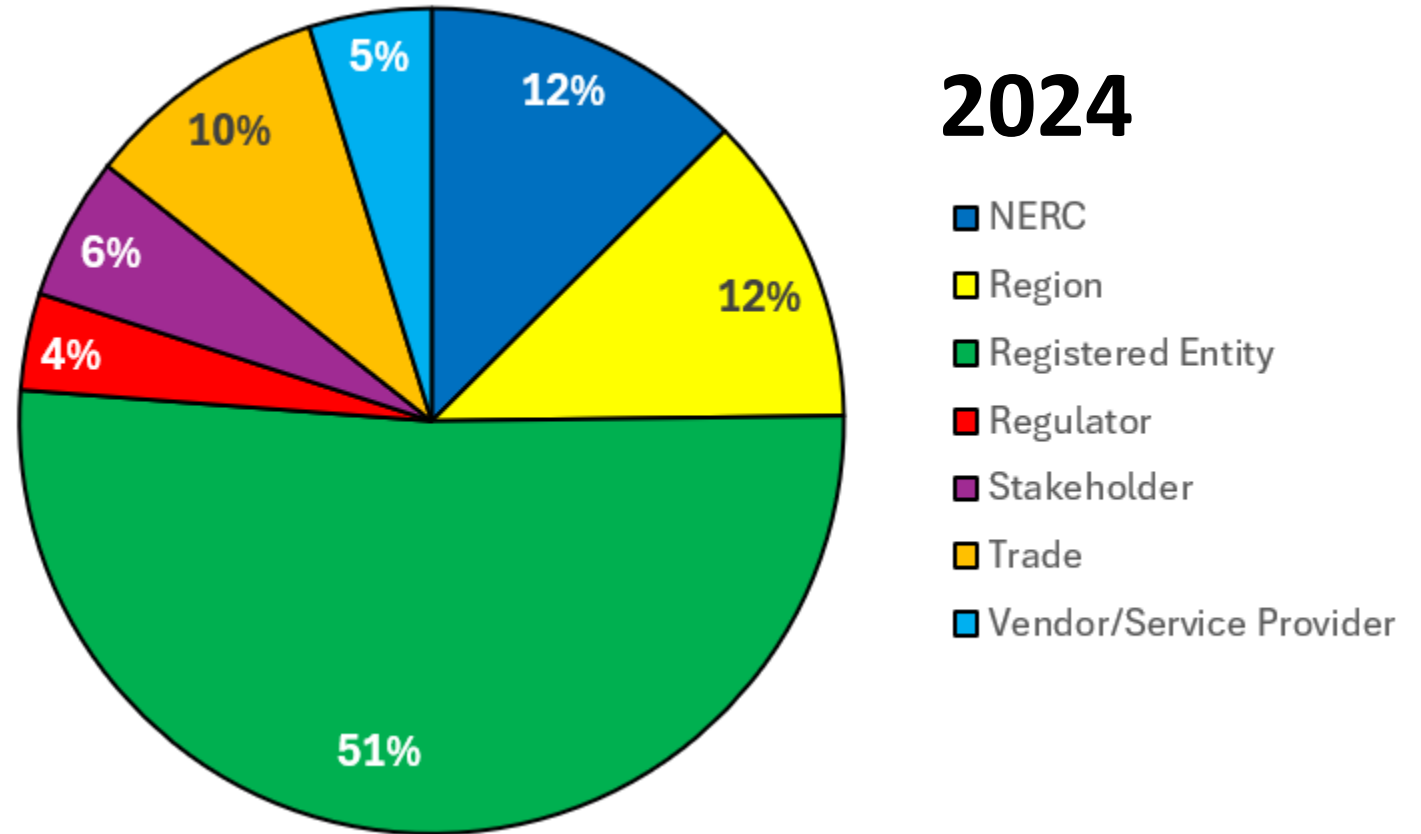
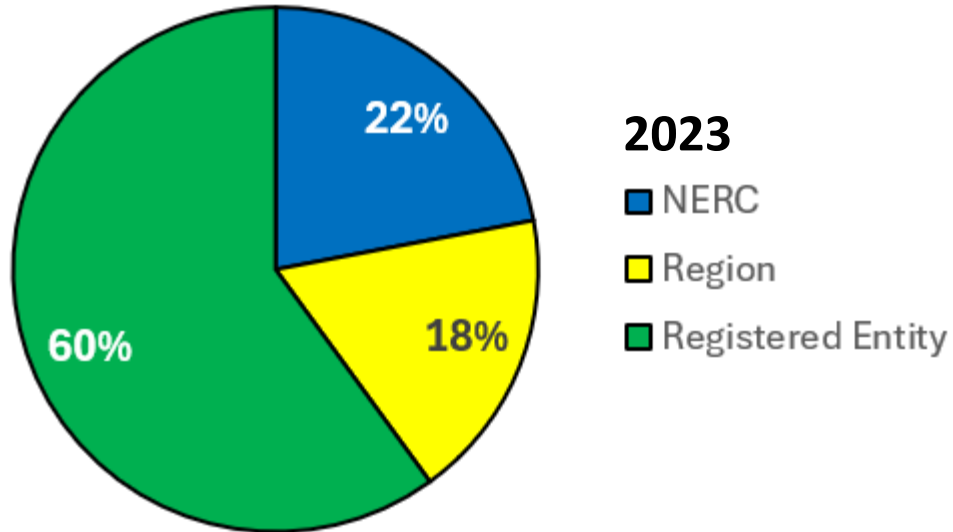
- Dec 2, 2024, though Jan 15, 2025

## Why

- To give our stakeholders a voice
- To learn what we are doing well and what we need to improve

**17%**  
**Increase in  
Participation**







# Help and Support

	Percentage Favorable or Neutral		Change
	2023	2024 (Current Year)	
NERC	80%	84%	Improved 4%
Registered Entity	71%	77%	Improved 6%
Region	53%	80%	Significantly Improved 27%
Regulator	No Data Submitted	85%	New Baseline
Stakeholder	Insufficient Sample Size (1)	81%	New Baseline
Trade	Insufficient Sample Size (1)	88%	New Baseline
Vendor/Service Provider	Insufficient Sample Size (1)	92%	New Baseline

# Technology Overall

	Percentage Favorable or Neutral		Change
	2023	2024 (Current Year)	
NERC	89%	93%	Improved 4%
Registered Entity	78%	83%	Improved 5%
Region	55%	82%	Significantly Improved 27%
Regulator	No Data Submitted	83%	New Baseline
Stakeholder	Insufficient Sample Size (1)	79%	New Baseline
Trade	Insufficient Sample Size (1)	88%	New Baseline
Vendor/Service Provider	Insufficient Sample Size (1)	90%	New Baseline

# What was on our customers' minds in 2023?



What was on  
their minds  
in 2024?



## Identified focus areas...

- Resolving issues faster; responding more quickly to reported issues
  - Increase focus on monitoring performance in real-time
  - Work with our Quality Assurance team to analyze trends
- Better informing our customers about the status of their issue
  - More messaging and notifications regarding status
- Making sure our solutions resolve the issue
  - Added emphasis on knowledge base and training
  - Improve team information sharing and collaboration

## ... and what we did.

*Emphasized prevention combined with proactive monitoring and trend analysis.*

*Emphasized need to contact customers throughout case lifecycle.*

*Increased use of Knowledge Base, promoted training resources, met with other functional areas (e.g., App Dev, Infrastructure) to share knowledge and experiences.*



- Making it easier to submit issues
  - Online tool for submitting cases (Assist Me)
  - And a 24 x 7 Outsourced Call Center
- Better informing our customers about the status of their issue
  - Assist Me outbound communications
- Resolving issues faster, and making sure our responses resolve the issue
  - Training, information sharing, Knowledge Base, Self-help, and feedback

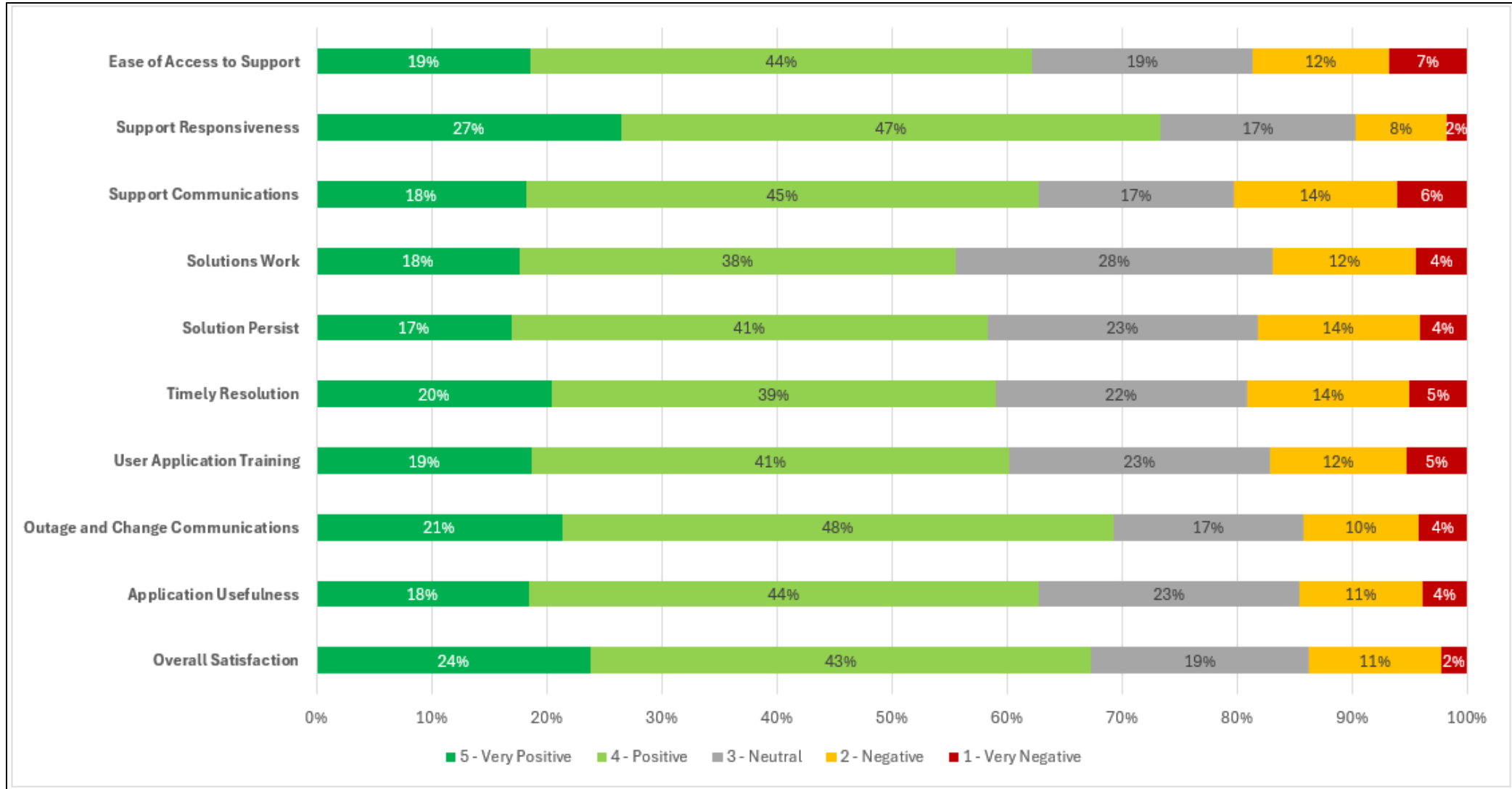


# Questions and Answers



# **Additional Information**





## **E-ISAC Operations**

### **Action**

Update

### **Summary**

The E-ISAC remained vigilant and maintained heightened awareness throughout the 2024 holiday season and U.S. inauguration. It shared rapid electricity sector context about a variety of individual cyber and physical incidents, though there was no specific, credible, 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.

The threat landscape remains unchanged. 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. The significant media coverage and uptick in unusual drone sighting reports was also closely monitored for industry.

Matt Duncan will summarize the E-ISAC's recent activities and the threat landscape for the Board of Trustees in this open session, with a focus on a brief discussion of the incidents over the holiday season, Chinese cyber activity, and drones. A comparison of 2024 and 2023 cyber and physical direct shares, a proactive E-ISAC program to address visible vulnerabilities, is included in this document.

Bluma Sussman will report on upcoming 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.

### **People's Republic of China (PRC) Cyber Threats**

People's Republic of China attributed cyber espionage activity continues unabated in the United States and internationally. The E-ISAC continues to monitor open sources, collaborate with government, identify vulnerabilities, and proactively hunt for threats in various sensor platforms including CRISP, Neighborhood Keeper, and other available intelligence sources.

In December, the E-ISAC provided members with a summary and overview of tradecraft used by PRC cyber threat actors, and others. Already the E-ISAC observed examples of attributed PRC tradecraft reported in January signaling continued activity.

Multiple PRC attributed cyber events impacting the United States include the discovery of a Chinese actor compromise of the Department of Treasury, specifically the Committee on Foreign Investment in the US (CFIUS). CFIUS scrutinizes real estate sales near US military bases and business deals for national security implications and a valuable espionage target.

Working with government and Energy Threat Analysis Center (ETAC) partners, the E-ISAC continues to assess the activity and impact associated with Salt Typhoon in the telecommunications sector. The successful compromises during previous Volt Typhoon and Salt Typhoon campaigns have demonstrated that PRC actors are a credible threat to the electricity industry. On the international scene, it has been reported that Chinese attributed cyber activity has doubled targeting Taiwan, and the Japanese police disclosed a campaign assessed to be conducted by the Chinese People's Liberation Army targeting intellectual property of Japanese companies. The E-ISAC asks that members please remain vigilant for malicious cyber activity during this time and continue to share information on potential PRC espionage activities.

### **PRC Threat Tradecraft and Techniques**

It is worth noting the tradecrafts and tactics used by the PRC actors, as they signal potential areas for collaboration and investment for industry. PRC cyber threat actor methodology begins by exploiting known vulnerabilities in public-facing applications that are end-of-life or unpatched. This initial access is conducted through exploitation of vulnerabilities in VPNs, firewalls, remote access tools, web-based application flaws, and brute forcing of credentials. Additionally, PRC threat actors commonly use these exploitation methods to build networks that provide obfuscation and a way to bypass geolocation. The E-ISAC is working with the Downstream-Natural Gas ISAC to evaluate this threat in the broader energy sector.

The next stage after initial access is to maintain persistence on victim networks. PRC threat actors use common webshells as well as customized malware. These actors then move laterally through victim networks using tools native to the environment such as Microsoft's PowerShell, Scheduled Tasks, Windows Management Instrumentation Consol (WMIC.) They also harvest legitimate user credentials and/or generate "super users" for themselves. These tools and methods allow PRC threat actors to "live off the land" and avoid detection. For example, the Salt Typhoon actors stole records from telecommunications companies, including data about where, when and whom customers of the compromised networks are communicating. The threat group also compromised private communications, including audio and text content, of targeted individuals who are primarily involved in government or political activities. Access to this information enables more sophisticated social engineering, such as voice phishing, SMS-phishing, and generative AI impersonation to obtain legitimate credentials from unwitting users.

The E-ISAC shared a preparedness guide with industry in November 2024 that highlighted electricity specific actions industry can take to prepare for PRC tradecraft, such as:

- Review thresholds for activating cyber incident response plans and consider exercising
- Review latest reports on China-linked adversary capabilities and tradecraft
- Baseline remote access controls and closely monitor remote connectivity to OT networks
- Backup critical IT and OT systems and maintain gold copies of configuration settings, especially for Energy Management Systems (EMS)
- Lower the threshold for reporting anomalous cyber activity to the E-ISAC and government
- Prepare for IT, OT and energy equipment supply chains to be disrupted in the worst-case
- Invest in resilient communications capabilities

## **Unusual Drone Activity**

The increased media scrutiny and awareness of unauthorized flights by Unmanned Aircraft Systems (UAS), or drones, near critical infrastructure in December 2024 further highlighted the potential risk to North American electric utilities. During this period, the E-ISAC experienced an unusually high volume of reports regarding suspicious drone activity, correlating with the media coverage of drone sightings in New Jersey as well as other states. To provide context, the number of drone incidents reported in the month of December represents almost half of drone related incidents reported to the E-ISAC in a two-year period. The incidents reported to the E-ISAC spanned 11 states, however none impacted the grid or operations. The E-ISAC recognizes that the increase in national reporting on suspicious drone flights is creating a heightened awareness of drones in general and is likely driving increased sharing.

The E-ISAC recently provided members with comprehensive physical security guidance and the results from its two-year drone pilot program, outlining key procedures and actions for utilities to enhance site and operational security, including recommended measures for responding to UAS overflight sightings. Additional data collected over time and investment in analysis of drone tactics, capabilities, and surveillance will assist in assessing normal vs. abnormal drone activity and aid in identifying intelligence gaps, emerging trends, and mitigation efforts. These efforts will enhance the E-ISAC's ability to provide valuable insight and meaningful analysis on the risks of drones to the electric industry despite current statutory and regulatory restrictions on the private sector for the interdiction of unauthorized drones.

## **2024 Direct Share Program Update**

As discussed at the August 2024 open committee meeting, adversaries continue to exploit both physical and cyber vulnerabilities in the industry's defenses. Regardless of whether the threat comes from the PRC, ransomware actors, hacktivists, or extremists, all malicious actors tend to exploit the same basic vulnerabilities. The E-ISAC uses its direct share program to spot gaps proactively on behalf of industry using a variety of tools and sources and share actionable mitigations with industry and cross sector partners when they are detected. Over the past several years, the E-ISAC formalized its monitoring program to provide direct shares of actionable intelligence to members and partners. Direct shares inform stakeholders of data breaches or leaks, cyber and physical security threats, potential vulnerabilities, and mitigation recommendations specific to their organization.

From January 1, 2024, through December 31, 2024, the E-ISAC sent 748 direct shares to electricity industry asset owner or operator (AOO) member organizations, an overall increase of 2.3 percent. Of the AOO member organization recipients, about 70 percent were small and medium utilities. Additionally, 2,790 shares were sent to interdependent E-ISAC partners (e.g. the other critical infrastructure sectors, government partners) during the same period, a decrease of 6.5 percent. The decrease in sharing with partners reflects a renewed focus on the electricity and gas industries and their equipment, and improved email security.

In 2025, E-ISAC will continue to invest in growing and refining this capability to include lower levels of vulnerability severity and greater coverage of social media and the dark web where credentials are often sold or leaked.

## Stakeholder Experience/User Experience

The E-ISAC stakeholder experience impacts every one of our 1800 member and partner organizations. Over the last year, the E-ISAC has been engaged in a robust stakeholder experience effort to continue increasing the value of the products, programs and services provided to the E-ISAC community. The work being completed as part of this stakeholder experience effort is also aligned to the E-ISAC's 2025 Work Plan Priorities and the 2026-2028 NERC Strategic Plan.

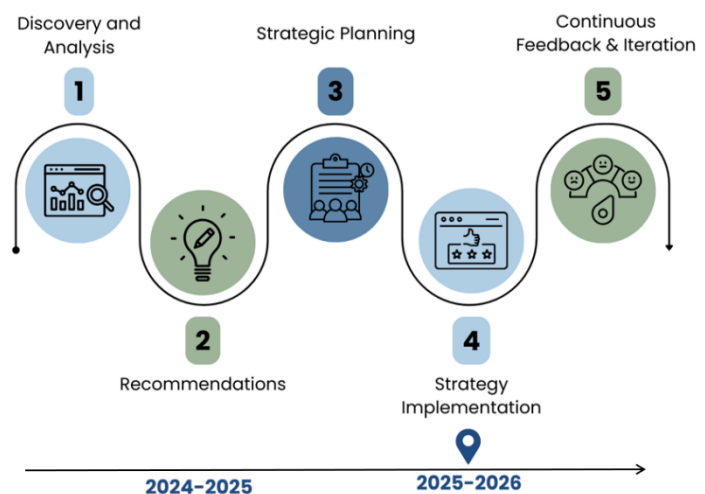
Since the project began last year, the E-ISAC has completed the initial two phases of the project, which include the initial discovery and recommendation phases. Leveraging Portal user trends, profile information, and behavior data, and in conjunction with consulting firm Main Digital, the E-ISAC developed tools such as stakeholder personas and service blueprints. A user experience evaluation of the E-ISAC Portal was also conducted, which included specific recommendations to elevate user experiences on the E-ISAC Portal, the primary digital platform.

The recommendations, which form the basis of the Strategic Implementation phase, are focused on optimizing and improving the following elements of the stakeholder experience:

1. **Content reach** for existing stakeholders—is the content targeted and reaching the right stakeholder groups?
2. **Content impact** for existing stakeholders—does the content provide stakeholders with the information they need to raise awareness, make decisions, take actions?
3. **User experience** for existing stakeholders—do E-ISAC products, programs and services provide value, across stakeholder groups, at each point in the stakeholder journey?
4. **Membership conversion rate** for targeted prospects—is the E-ISAC effectively engaging with new members to strategically expand the E-ISAC community?

## Strategic Implementation Phase

This past fall, the team conducted the Strategic Planning phase. This process resulted in the creation of a prioritized and sequenced set of activities aligned to the key action areas. Equipped with this set of strategic priorities, the E-ISAC is well poised to begin the Strategy Implementation phase which will run through 2025 and into 2026. This phase is focused on implementing the recommended actions and maturing the current state E-ISAC customer experience to an elevated customer experience. Main Digital's expertise will continue to be leveraged throughout the strategy implementation phase of the project. Their role will entail overseeing comprehensive adoption of recommendations across the E-ISAC and providing an independent assessment of E-ISAC products with actionable recommendations to improve content quality, relevance, and impact.



Main Digital is contracted to provide design and development services for the E-ISAC Portal and Public websites in 2025. Under this contract they will implement user experience (UX) design

changes to those websites through 2025. User experience enhancement activities aim to improve the navigation, intuitiveness, and aesthetics of the E-ISAC's primary digital delivery channels such as the E-ISAC public website and marketing emails. Additionally, the E-ISAC will also explore channels such as digital chat micro communities that leverage digital chat tools like Slack, Signal, or Teams to quickly communicate with credible and trusted analysts across the industry.

The E-ISAC has recently implemented several Stakeholder User Experience updates including:

- **Implementation of the ESCC Directory** on the E-ISAC Portal—a recommendation out of GridEx VII to address the resilient communications needs of the ESCC
- **Simplification of Portal Terminology and Menu Navigation**—based on stakeholder feedback to streamline terminology and make navigating and search easier
- **Migration of CRISP Analysts' Reports** from the Government-supported legacy platform to the E-ISAC Portal for seamless reporting access and greater integration with member organizations' threat intelligence platforms

Throughout the Strategic Implementation phase, the E-ISAC and Main Digital teams will measure and assess progress across information sharing, information consumption, event participation, and stakeholder sentiment factors. The E-ISAC will use measures such as email open rates, content viewership rates, event participation rates, security information sharing rates, sentiment ratings, and key impact survey responses. Progress will also be measured against current baseline data on E-ISAC member and partner engagement and participation, to inform strategic engagement for increased participation and involvement in E-ISAC programs and services. As part of this phase, the E-ISAC will also develop a comprehensive strategy to operationalize stakeholder feedback and iterate E-ISAC products and programming.

### **Strategic Engagement Opportunities**

Strategic engagement is another significant aspect of the E-ISAC stakeholder experience and there are substantial opportunities to generate maximum impact and value for the E-ISAC community. Strategic engagement efforts will be aligned to the E-ISAC's strategic membership growth and engagement goals and will focus on providing timely and relevant information for participants as well as a high-quality stakeholder experience. This year, the E-ISAC will focus strategic engagement efforts towards increasing membership across: Small and Medium Utilities, IBRs, NERC Registered Entities, and the Vendor Affiliate Program Partners. This includes: attending in APPA's Joint Action Agency (JAA) Conference, to encourage membership participation and information sharing across small and medium public power utilities, briefing at NRECA's DistribuTECH about GridEx to encourage cooperatives to exercise their response capabilities, participation at renewables conferences such as SolarPlaza to talk about the value of E-ISAC for the renewables community, and strategic outreach with OEM and security vendors to facilitate further collaboration and discussion around issues like supply chain and ransomware.

## Special Events

We experienced record-breaking attendance at GridSecCon 2024, hosting over 700 attendees, marking a 33% increase from 2023. Participants rated speakers and content an average of 4.5 out of 5 stars.

GridSecCon 2025 will be October 7–10 at the MGM Grand in Las Vegas and will build on the successes of GridSecCon 2024 and participant feedback.

And GridEx VIII, North America's largest grid security exercise, will be November 18–19, 2025.



## Partnerships and Collaborations

In addition to large scale events such as GridSecCon and GridEx, the E-ISAC continues to increase its collaboration with key partners to enhance value for our members. Recently the E-ISAC implemented a three-year strategy with the European and Japanese Electricity ISACs to operationalize our Memorandum of Understanding and strengthen international information sharing. The E-ISAC also expanded the Vendor Affiliate Program to address supply chain interdependency challenges and provide information and ongoing benefits to industry members, including a new partnership with the SANS Institute to offer world-class training and actionable resources to qualifying E-ISAC members.

The E-ISAC also maintains critical partnerships with Canadian industry and government, as well as other ISACs across critical infrastructure sectors. E-ISAC staff regularly engage in person and virtually with Canadian counterparts at Electricity Canada, Natural Resources Canada (NRCAN), Canadian Centre for Cyber Security (CCCS), Public Safety Canada, Royal Canadian Mounted Police (RCMP), and Canadian Gas Association (CGA) to broaden collaboration and information sharing. E-ISAC leadership continue to participate in Canadian sector partnership coordination forums like the Energy Sector Advisory Committee and events like GeekWeek and tabletop exercises. Within the U.S. critical infrastructure cross-sectors, the E-ISAC maintains close partnerships, including formal information sharing agreements with the DNG-ISAC, ONE-ISAC (formerly ONG-ISAC) and MS-ISAC, Communications ISAC, Water-ISAC, as well as engagement with the Tri-Sector, and, regular participation and collaboration with the Electricity Subsector Coordinating Council (ESCC).

Additional work to improve the stakeholder experience will continue, not just into this next year, but as an ongoing and critical consideration which is layered over every Portal post, marketing message, program agenda and engagement. The E-ISAC is focused on making sure that its members and partners derive meaning and value from its products and services as we work together to protect and defend our nation's critical infrastructure and reduce risk of cyber and physical security threats to the electricity industry.





# E-ISAC Operations

Matt Duncan, VP, Security Operations and Intelligence  
Technology and Security Open Meeting  
February 12, 2025

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY





### People's Republic of China (PRC) Cyber

- U.S. Dept of Treasury hacked
- Continued activity by Salt Typhoon
- Cyber espionage against Taiwan and Japan

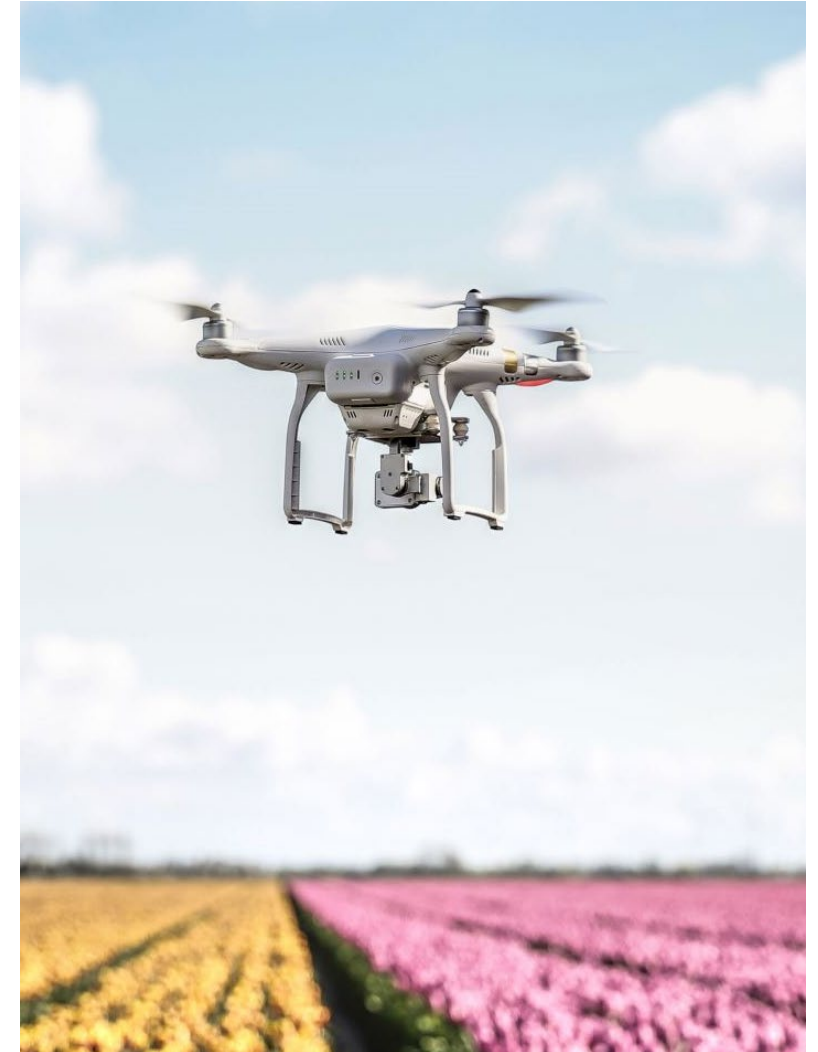
### Holiday Vehicle Extremist Events

- No threat to grid or BPS, however tactics of concern

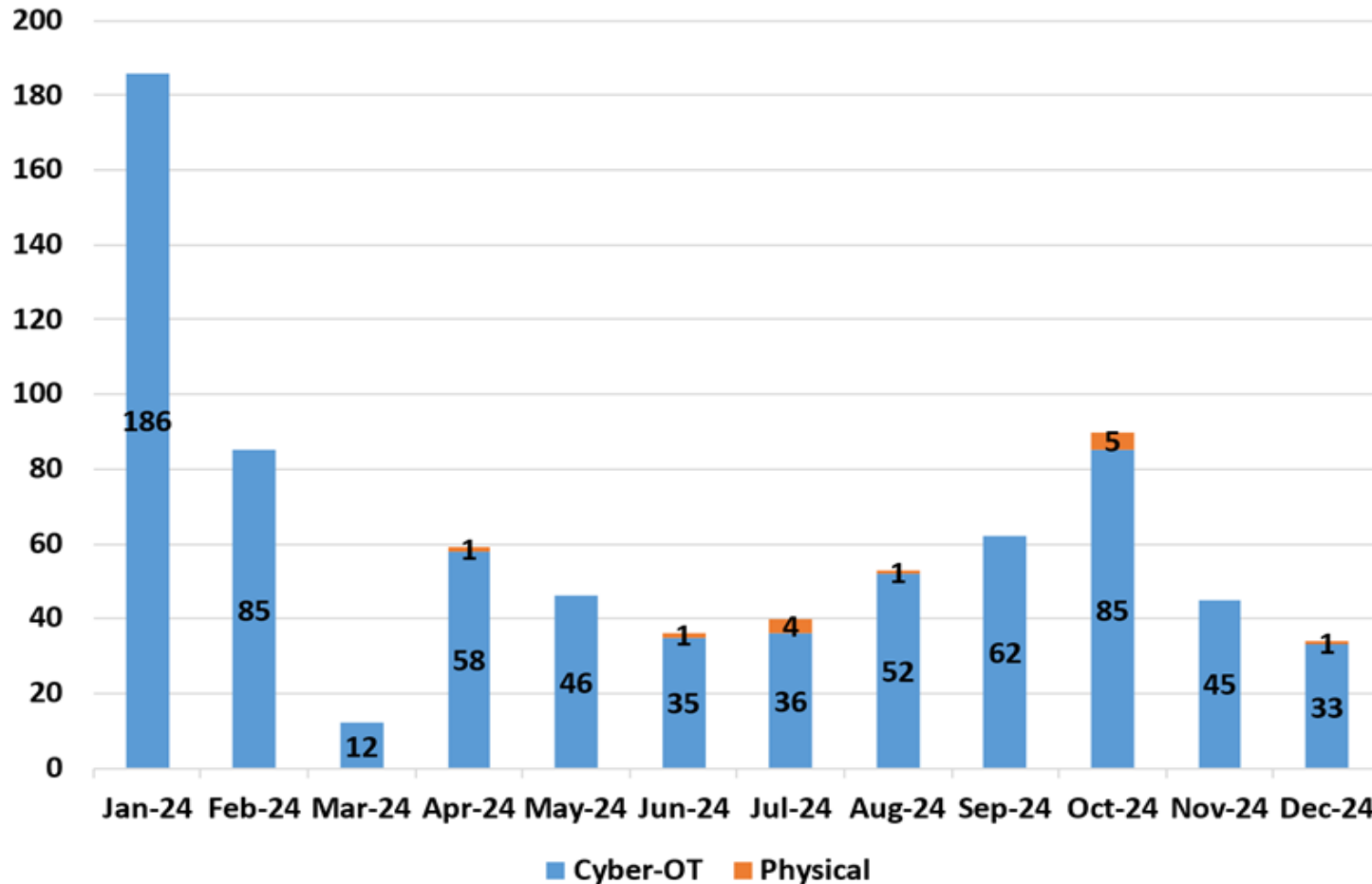
### Vulnerabilities, Tech Baseline, Credentials

- Firewalls, end of life equipment, business email compromises

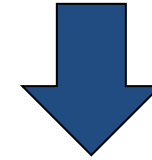
- Uptick in reports of unauthorized drone flights but no impact to the BPS or grid
- Media attention has driven increased reporting
- **E-ISAC Drone Tools**
  - Comprehensive guidance on reporting unauthorized drones
  - Key procedures and actions for utilities to take
  - Two-year pilot report, data, and recommendations
- **Future Actions**
  - Exploring future drone data collection efforts



## 2024 Direct Shares Rolling 12 Months



**748 proactive direct shares**



**527 member organizations**

Direct shares inform members/partners of:

- data breaches or leaks
- cyber and physical security threats
- potential vulnerabilities

Each share contains mitigation recommendations specific to their organization and vulnerability



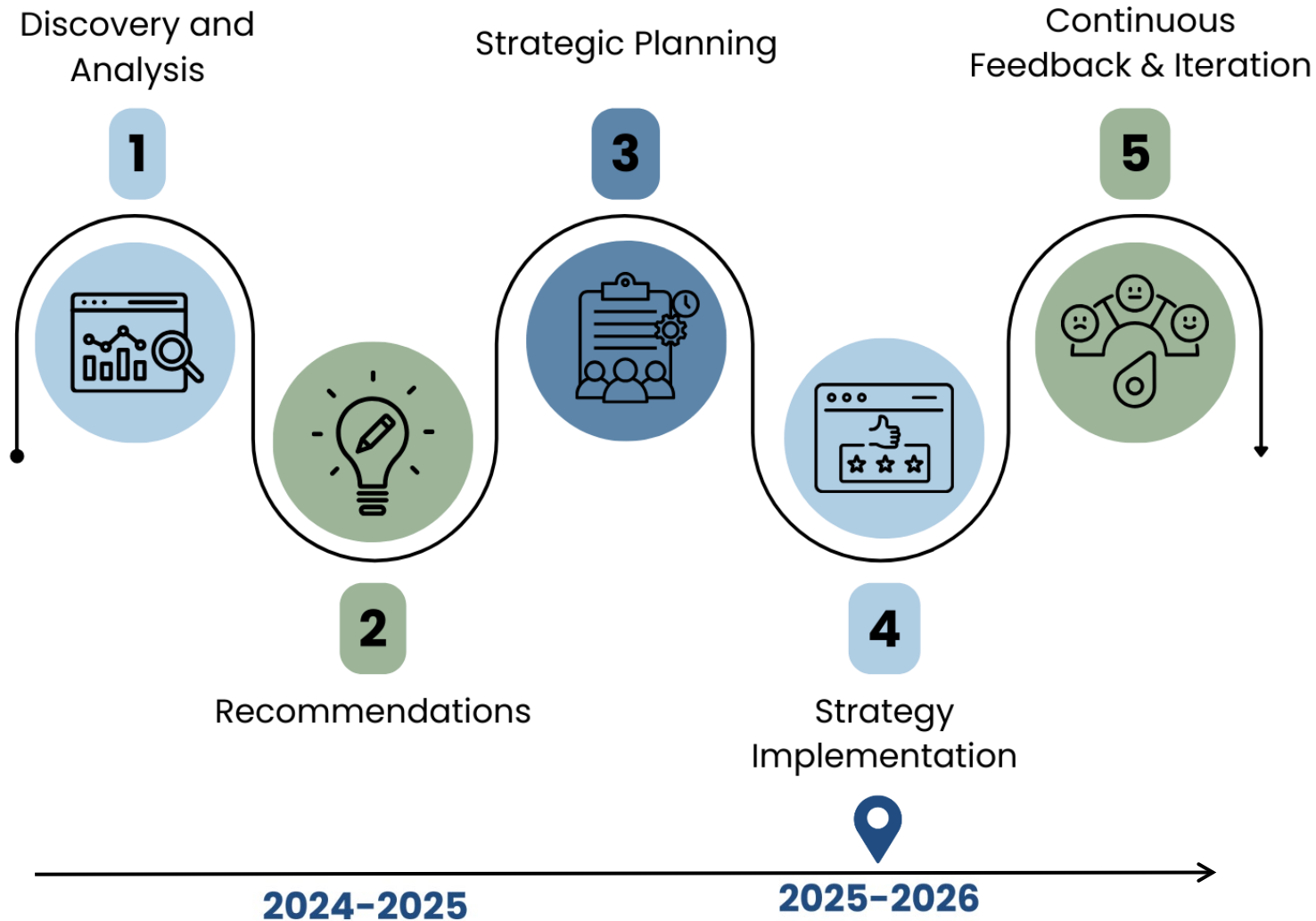
# E-ISAC Stakeholder Experience


Bluma Sussman, VP, Stakeholder Engagement  
Technology and Security Open Meeting  
February 12, 2025

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY






PostsDAOESCC DirectoryAutomated Information ExchangeSupportSearch...username

Home > DAO - Faraday Energy

**Faraday Energy**  
Profile  
Contacts  
ESCC List

**Agreements & Reviews**  
✓ DAO User Agreement  
✓ Organization Review

DAO - Faraday Energy  
**Profile**  
Add New ContactEdit Org Profile

Designated Primary Admin / DAO  
Frederik Pohl

Organization Name  
Faraday Energy

Acronym

Phone  
(703) 777-7777

Website  
N/A


Parent Organization  
N/A

Organization Record Type  
Member

Physical Address  
3333 Maple Avenue  
Centerville, Georgia 78092  
United States

Description  
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris.

▼ E-ISAC Member Details

Bulletin

Author: E-ISAC Org: E-ISAC Group: E-ISAC  
9/13/2024 12:46:23 PM UTC

TLP: Green – Do NOT share on publicly accessible sites or with the media. Limited disclosure, restricted to that community.

**CYBER THREAT INTEL REPORT**  
**CyberAv3ngers Conducting Reconnaissance Against ICS/OT Entities and Devices in June and July 2024**  
According to an E-ISAC Partner's report published yesterday, in June and July of 2024, hacker CyberAv3ngers performed research and reconnaissance against Industrial Control Systems (ICS) / Operational Technology (OT) entities and devices using Stark Industries Solutions LTD infrastructure, a bulletproof hosting provider. They assess with moderate confidence that this activity is used to scan and collect information from targeted entities to include a U.S. energy sector company, industrial automation companies, and a thermal engineering company. Certain Internet-exposed devices were targeted to include Siemens S7, CIMON Automation, and devices running OPC Unified Architecture Server, Omron Factory Interface Network Service (FINS), and CODESYS protocols. Although these protocols overlap with those targeted by PIPEDREAM and CHERNOVITE, investigation continues. Additionally, this is the first time our partner has discovered CyberAv3ngers performing reconnaissance against t...  
[To view the entire bulletin, log in to the E-ISAC Portal](#) [View this bulletin as a web page](#)  
**For more information or assistance:**  
Email [operations@eisac.com](mailto:operations@eisac.com) Call the E-ISAC 24x7 Hotline at 202-790-6000  
[Manage your notifications](#)



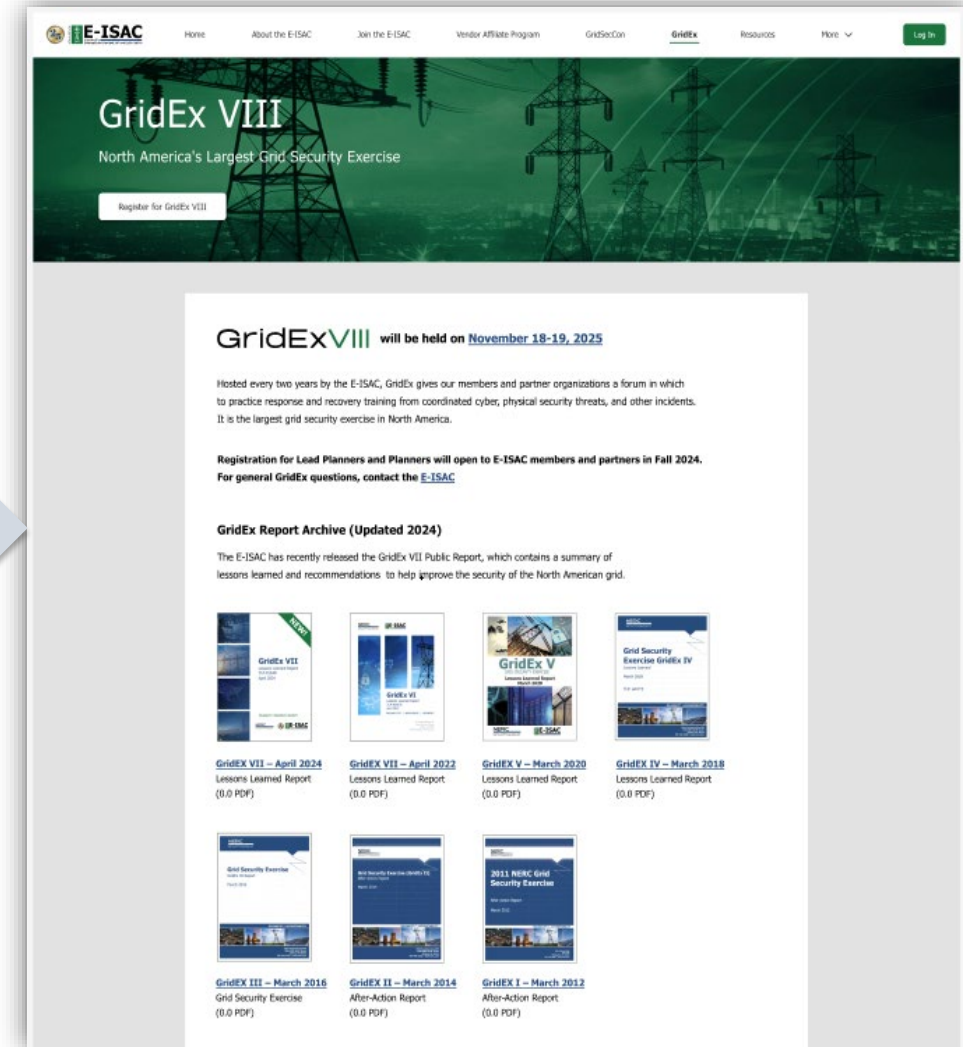
Notifications  
by Persona

Persona  
Based Portal  
Experiences

Consider  
Enhanced  
Mobile  
Experience

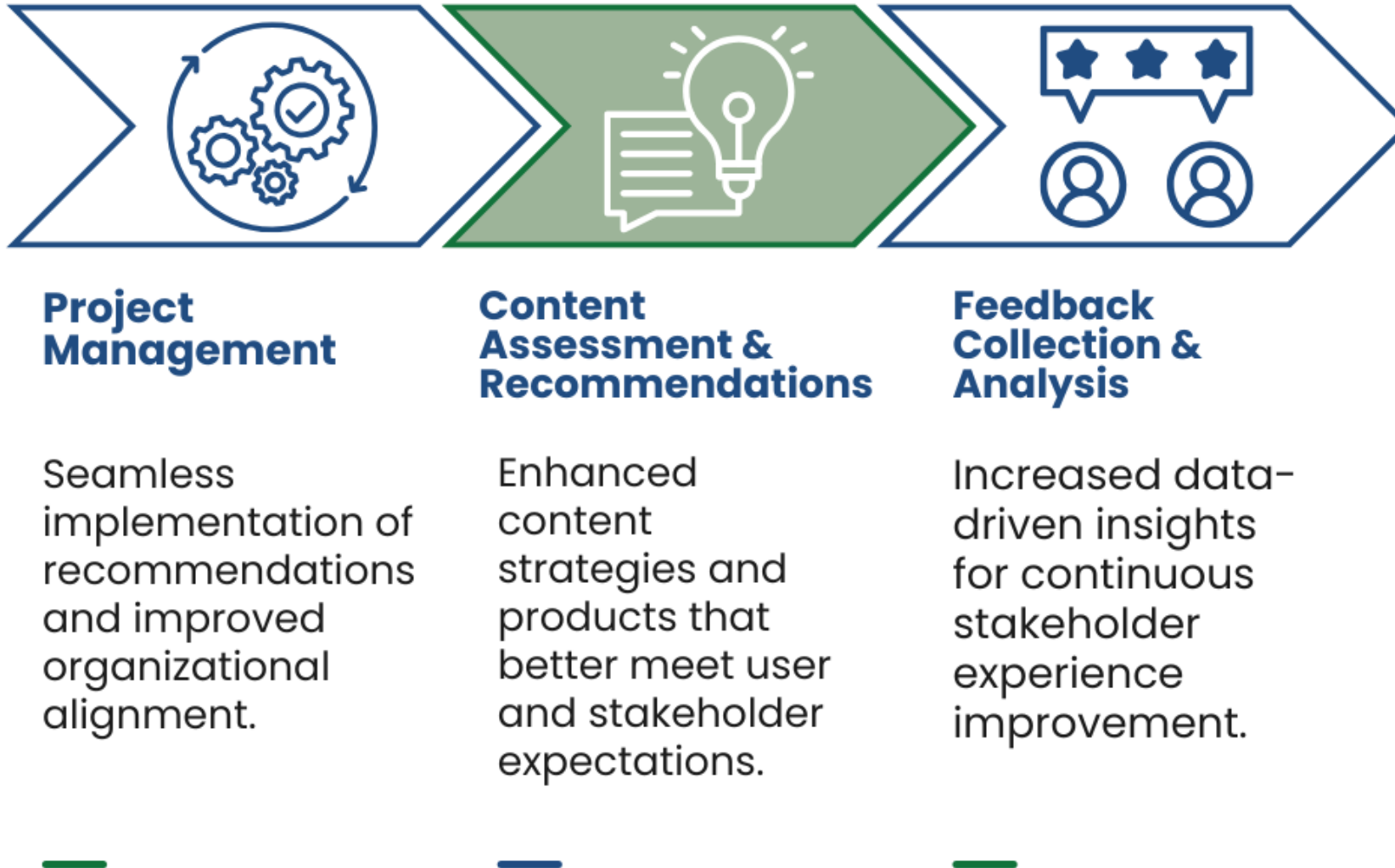
Targeted  
Public Site  
Redesign

Explore Micro  
Communities











# Questions and Answers