A DIVISION OF NERC
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

2023 E-ISAC END-OF-YEAR REPORT

TLP:CLEAR

MESSAGE FROM THE CHIEF EXECUTIVE OFFICER

MANNY CANCEL

Looking back at 2023, I am impressed by the resilience of an electricity industry that faced relentless cyber threats, increased targeting of infrastructure, and a complex geopolitical environment. Despite those challenges, industry worked together to keep the lights on for more than 400 million North Americans.

The E-ISAC gave our nearly 1,800 member and partner organizations the tools to stay ahead of the challenges. We expanded the quality of our analysis, streamlined information sharing, and strengthened partnerships.

Cybersecurity Risk Information Sharing Program (CRISP) data and threat hunts identified malicious traffic and monitored extremist chatter threatening electricity assets, and we prioritized the most critical threats to deliver timely, relevant analysis. E-ISAC products kept members current on physical security threats, while Vulnerability of Integrated Security Analysis (VISA) workshops and other programs equipped industry with security best practices.

The E-ISAC participated in more than 175 conferences, briefings, and other events, sharing insights and exchanging ideas. GridSecCon and GridEx–our flagship events–drew praise from participants, while our Industry Engagement Program (IEP) brought professionals together to collaborate on best practices.

New programs addressing real world events were introduced. The debut of the Physical Security Regional Workshop series in Charlotte, North Carolina, brought together more than 100 industry and government attendees; more security workshops will follow in 2024.

We focused on gathering feedback, building a community of trust, and growing our people-first culture.

E-ISAC member organizations, which grew by 11%, shared valuable security information throughout the year. Strong relationships with our partner organizations helped industry collectively reduce risk; in particular, activities with U.S. and Canadian government partners reached their highest levels ever. These insights, coupled with expertise through initiatives like the Vendor Affiliate Program (VAP), kept industry ahead of the threat curve.

Community feedback resulted in us introducing streamlined information sharing processes, updated automated sharing capabilities, and E-ISAC Portal improvements.

While we had much to be proud of in 2023, we're looking ahead to 2024. This includes celebrating 25 years of providing industry leadership and collaboration and CRISP's 10th anniversary. As we recognize these milestones, I am reminded the E-ISAC only exists because of our members and partners.

Thank you to E-ISAC staff for your dedication to the security of the power grid. The E-ISAC owes a debt of gratitude for the unwavering support of the North American Electric Reliability Corporation (NERC), the Electric Reliability Organization (ERO) Enterprise, the Member Executive Committee (MEC), the NERC Board of Trustees, and the Electricity Subsector Coordinating Council (ESCC).

I look forward to working together to maintain a reliable, resilient, and secure North American grid.

Manny Cancel

SECTION 1

The Evolving Threat Landscape and the E-ISAC's Response

The E-ISAC equipped industry with 24/7 information and analysis to keep infrastructure secure from physical and cyber security threats.

China: The Preeminent Threat in an Unpredictable World

The global geopolitical situation grew even more complex, with increased implications for the North American power grid. The E-ISAC assessed the People's Republic of China (PRC) as a top cyber espionage adversary. China threat actors demonstrated increasing sophistication and adaptive techniques. State-sponsored cyber threat actor Volt Typhoon drew notable concern because it specifically targeted U.S. infrastructure.

37 China-related cyber events documented by the E-ISAC

China was not the only advanced persistent threat in 2023:

- Russia employed advanced attack capabilities, including espionage and influence campaigns.
- Iran's cyber capabilities grew as did its willingness to conduct aggressive operations.
- North Korea remained a sophisticated and agile threat, with activities focused on espionage and cybercrime.

Constant Vigilance, Rapid Response, Deep Analysis

The E-ISAC's security response approach focused on threat monitoring and rapid communication of information. The E-ISAC Watch provided 24/7 monitoring of the dark web, criminal forums, and industry internet-facing connections, identifying potential ransomware threats, third-party compromises, and unintended unsecured infrastructure. All-Points Bulletins offered immediate updates, while analysis on events such as continued Russian espionage activity and the Israel-Hamas conflict and their potential ramifications on grid security provided context.

The Watch had 703 proactive direct shares with E-ISAC members in 2023

Advanced Intelligence

Members and partners had access to advanced information and trends through the E-ISAC's intelligence expertise and reach across industry. For example, **CRISP's** unique data collection capabilities equipped industry with the knowledge to detect cyber attacks. The E-ISAC's role in the Energy Threat Analysis Center (ETAC), a Department of Energy-led program, affords access to advanced intelligence information about emerging threats.

> "The E-ISAC provides great access to actionable intelligence, which helps drive our security efforts."
>
> E-ISAC Member Organization

Physical Security Threats a Top Concern

Protecting physical infrastructure from a wide range of threats continued to be a top priority in 2023. Threat levels stayed elevated throughout the year with more than 2,800 physical security incidents shared with the E-ISAC, including ballistic damage, theft, and vandalism. Of that number, approximately 3% resulted in varying levels of impact to the electricity grid.

Opportunistic Domestic Violent Extremists (DVE): DVEs aimed to exploit potential social unrest such as political elections (including the upcoming 2024 election), economic issues, and activistic causes to target infrastructure.

Growing Threats of Unmanned Aerial Vehicles (UAV): With the rapid technological expansion of UAVs such as drones, utilities faced potential risks for surveillance and attacks.

Insider Threats: Individuals with access to sensitive systems presented risk to critical infrastructure.

Additional Risks: Theft, accidents, and other incidents posed additional threats.

E-ISAC Provides Context

Members and partners made sense of the chaotic security landscape with the help of E-ISAC products such as weekly and quarterly reports that provided threat updates. Additional insights were offered by products such as the E-ISAC's drone pilot program and the Physical Security Resource Guide. The member-driven Physical Security Advisory Group also contributed to the collective knowledge base.

Strong Information Sharing Partnerships

The E-ISAC's proactive partnerships produced valuable security information, as sharing activity with federal and Canadian partners reached the highest ever levels in 2023. In particular, the E-ISAC engaged in multiple intelligence initiatives with the FBI and National Counterterrorism Center.

Vulnerability of Integrated Security Analysis (VISA) Workshops

A resource unique to the E-ISAC, VISA Workshops teach participants how to effectively assess the vulnerabilities of a site's critical assets.

7 VISA workshops conducted in 2023

> "The VISA process builds incredible advocacy for physical security. It builds bridges across many workgroups to better protect infrastructure."
>
> VISA Workshop Participant

Operators Face Daily Threats to OT and IT Systems

The electricity industry encountered an unprecedented number of sophisticated cyber vulnerabilities in 2023 such as malware, ransomware, supply chain exploits, and other risks.

↑2X Vulnerabilities have more than doubled from 2019 to 2023

↑24% Average increase in critical vulnerabilities from 2019 to 2023

Major Cyber Events

- **MoveIT Transfer:** Exploits a vulnerability in MoveIT Transfer to steal sensitive data.
- **Microsoft Outlook Privilege Escalation:** Zero-click vulnerability requiring no user interaction; enabled a Russian-based actor to conduct reconnaissance on government, energy, and transportation in Europe.
- **Citrix Bleed:** Successful exploitation allows attackers to bypass authentication methods; presents a high severity due to widespread use.
- **HTTP/2 "Rapid Reset" Zero-Day Vulnerability:** Zero-day vulnerability that enables distributed denial of service (DDoS) attacks on a scale never seen before.
- **Maximo Asset Management Vulnerability:** Wide use across the electricity industry increases risk; exploitation could cause business disruption.

2023 Cyber Shares from Member and Partner Organizations

968	240	254	123	110	241
Total	Vulnerability	Phishing	3rd Party Ransomware	DDOS	Other

Staying Ahead of the Curve

The E-ISAC helped members stay ahead of threats by highlighting critical information through "ACTION REQUIRED" Portal posts and vulnerability severity ratings. Products such as the Small and Medium Utilities Community Weekly Situation Report offered tailored information.

Hunting for Threats

E-ISAC threat hunts used CRISP data and other tools to produce more than 70 reports to help utilities identify attacks on infrastructure. Threat hunt reports also generated member information shares in response, further adding to the knowledge base.

Anticipating Future Threats

New technological advances such as artificial intelligence can spur positive innovation, but also the potential for large-scale risk. The E-ISAC will leverage CRISP, the Cyber Security Advisory Group of subject matter experts, and threat hunts to prepare members for future threats.

> "The E-ISAC provides awareness of events I might not otherwise know about."
>
> E-ISAC Member Organization

SECTION 2

Industry Leadership and Collaboration

GRIDSECCON 2023
NERC • E-ISAC • NPCC

GridSecCon 2024 will take place October 22-25 in Minneapolis, Minnesota.

GridSecCon Brings Industry Together in Québec City

The electricity industry gathered in Québec City in October for the first in-person GridSecCon since 2019. GridSecCon attendees engaged in world-class training sessions, gained insights from expert panels and keynotes on critical topics impacting industry, and enjoyed opportunities to network with industry peers. Once again, the Women's Networking Breakfast featured inspiring presentations from leaders in industry and opportunities to reflect, celebrate, and support women in the energy sector.

During the event, the E-ISAC presented the annual Electricity Security Service Award in honor of Michael J. Assante, which recognizes individuals or teams that have made significant contributions to support the security of the North American electricity industry. The 2023 Assante Award winners were: Jonathan Bransky, Dominion Energy; Steen Fjalstad, Midwest Reliability Organization (MRO); and Steve McElwee, PJM.

> "I really enjoyed the variety of topics covered, the expo, and the fantastic networking opportunities."
>
> GridSecCon Attendee

464 Attendees

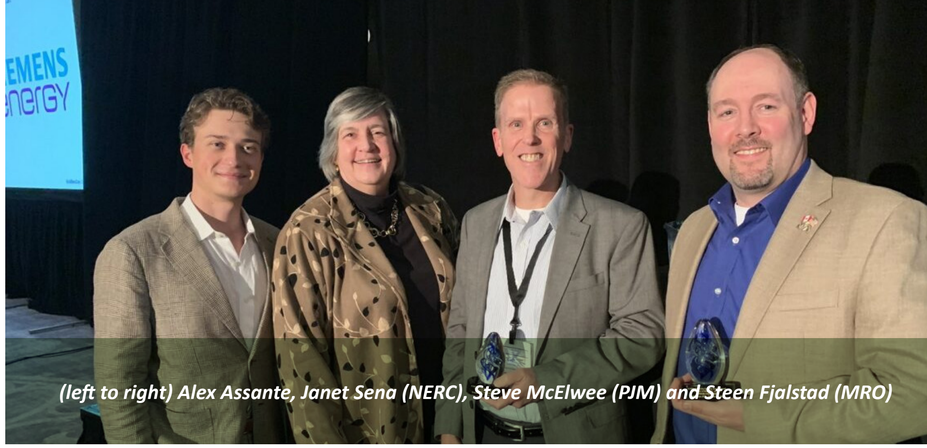
201 Organizations

92 Speakers

32 Sessions

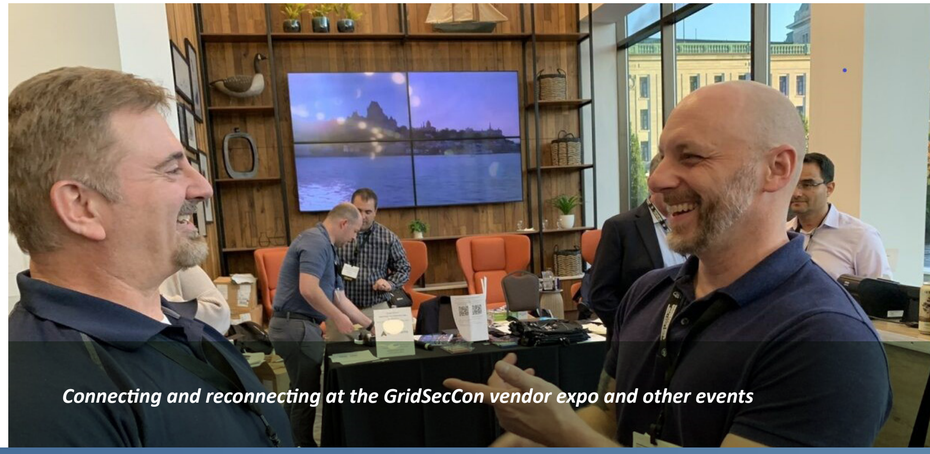
21 Exhibitors

20 Sponsors



(left to right) Alex Assante, Janet Sena (NERC), Steve McElwee (PJM) and Steen Fjalstad (MRO)

The Women's Networking Breakfast



Connecting and reconnecting at the GridSecCon vendor expo and other events

"GridEx VII was one of the best exercises I've ever been a part of."

GridEx VII Participant

"GridEx gave us the ability to test our teams in a collaborative approach…and tested our teams from a ground up perspective. "

GridEx VII Participant

"My players found the whole exercise helpful. The level of intensity helps them be prepared for the real events."

GridEx VII Participant

The GridEx VII executive tabletop

GridEx Strengthens Industry's Response

GridEx serves as the largest grid security exercise in North America. Held in November, GridEx VII Distributed Play prepared industry for real-world incidents by challenging participants to respond to and recover from a complex, real-world threat to the bulk power system. The GridEx VII executive tabletop, held at the E-ISAC's Washington, D.C., office, brought together top leaders in government, industry, NERC, the ERO Enterprise, and energy trade associations to discuss strategic and policy-level issues raised during the exercise. A public report of GridEx VII lessons learned outcomes will be available at the end of the first quarter of 2024.

15,000+
Estimated Participants

252
Organizations

230
Tabletop Participants

A Leading Voice for Grid Security

From conferences to the U.S. Capitol, the E-ISAC's perspective on security issues raised awareness about the electricity security landscape.

Participated in **175+** events

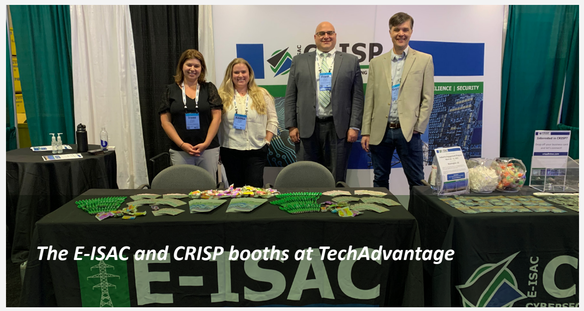
Physical Security Regional Workshop speakers

More than 100 electricity industry professionals attended the E-ISAC Physical Security Regional Workshop in October in Charlotte, North Carolina.

E-ISAC CEO Manny Cancel **testified** on security threats and the role the E-ISAC plays in grid security before the House Subcommittee on Oversight and Investigations, which is part of the Committee on Energy and Commerce, in Washington, D.C., in July.

The E-ISAC spoke at **32** conferences

Attendees at industry conferences learned the E-ISAC's insights on electricity security topics in keynotes, briefings, and panels.



The E-ISAC and CRISP booths at TechAdvantage

CRISP-hosted workshops in NYC and Washington, D.C., offered updates on the program, industry leader insights, and training sessions.

The E-ISAC gave updates on grid security and emphasized the importance of the U.S.-Canadian information sharing relationship at the Regie de l'énergie Annual Reliability Seminar, held by Québec's reliability coordinator, and other events in Canada throughout the year.

130+ Classified/unclassified briefings delivered by the E-ISAC at industry and government events

Members engaged in robust discussions and gained knowledge through E-ISAC-hosted monthly briefings and webinars, as well as in-person and virtual Industry Engagement Program (IEP) sessions.

IEP Participation

6	109	155
Sessions	Orgs.	Ind.

"This was a great venue for collaboration, bringing like-minded people together to talk about an important aspect of our business, and that's securing the grid."

Physical Security Regional Workshop Attendee

"I appreciated the overview of all of the E-ISAC's offerings. Getting the full picture is helpful for getting the most out of our partnership with the E-ISAC."

IEP Participant

Strong Partnerships Enrich Information Exchange

The E-ISAC worked with more than 300 U.S. and Canadian government agencies, private sector organizations, trade associations, and the ERO Enterprise to help industry collectively reduce risk.

U.S. Government Partners: Strategic partnerships with U.S. government agencies removed barriers to information exchange and improved the energy sector's collective security posture. U.S. government partners received information the E-ISAC gathered through its threat monitoring activities.

Canadian Partners: Engagement with Canadian partners such as the Canadian Centre for Cyber Security, NRCan, Public Safety Canada, Royal Canadian Mounted Police, and Electricity Canada played an important role in ensuring cross-border information sharing and strengthened relationships.

E-ISAC Partner Briefings

The E-ISAC conducted tailored briefings with a wide range of stakeholders, including the Director of National Intelligence, FBI, Pentagon Force Protection Agency, and Electricity Canada.

International Partners: Common security issues and interest in best practices resulted in an expansion of the E-ISAC's global engagements. In addition, the E-ISAC continued its partnership with the Japanese Electricity Information Sharing and Analysis Center (JE-ISAC) and European Energy Information Sharing and Analysis Center (EE-ISAC).

The E-ISAC held 23 presentations and meetings with international peers

ISACs: The E-ISAC regularly engaged with its ISAC partners to share best practices and discuss the impacts of threats, including the Tri-Sector working group consisting of the financial, communications, and energy sectors. These collaborative efforts led to products that increased security awareness for E-ISAC members.

Trade Associations: Partnerships with industry trade associations and the E-ISAC led to positive benefits for all stakeholders. The CEO-led ESCC highlighted the strength of these relationships through high-level collaboration.

"The E-ISAC … facilitates valuable information sharing amongst relevant energy partners."

E-ISAC Partner Organization

SECTION 3

A Trusted Information Sharing Community

The E-ISAC's nearly 1,800 member and partner organizations represent the largest information sharing community in the energy sector. More than 7,000 E-ISAC Portal users serve as the first line of defense for critical infrastructure. Members and partners can protect their assets, justify security investments, and save time by using E-ISAC products and services.

> "The E-ISAC is the gold standard for information sharing across the sector."
>
> E-ISAC Member Organization

1,769 Total Orgs.

13% Org. Growth

7,124 Portal Users

31% Portal User Growth

1,442 Member Organizations

11% Member Growth

527 NRECA Members

352 APPA Members

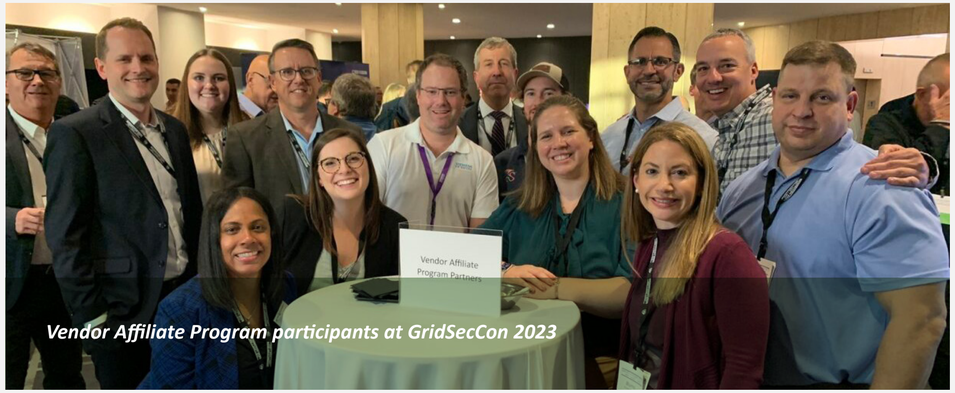
107 EEI Members

34 Electricity Canada Members

14 EPSA Members

327 Partner Organizations

16% Partner Growth



Vendor Affiliate Program participants at GridSecCon 2023

Vendor Affiliate Program Mitigates Risk to Industry Supply Chain

Original equipment manufacturer (OEM) and security vendors play a critical role in securing electricity infrastructure. The E-ISAC Vendor Affiliate Program gives participating organizations an opportunity to contribute to the industry's collective defense. Vendor participation in the E-ISAC community offers members access to the expertise and thought leadership of industry vendor organizations.

1898 & CO. · axio · DRAGOS · SEL Schweitzer Engineering Laboratories · Fortinet · Finite State · Itron · Nozomi Networks · Siemens Energy · 3B Protection Ballistic / Blast / Break-In · Google Cloud · Sargent & Lundy · Hitachi Inspire the Next · Hitachi Energy

Members Ask, the E-ISAC Delivers

Members shared their thoughts and ideas on how the E-ISAC could more effectively provide the quality security information they needed, when they needed it most. The E-ISAC responded by delivering a series of updates throughout 2023.

2023 Stakeholder Feedback Survey

The E-ISAC's Stakeholder Feedback Survey, conducted in partnership with J.D. Power, yielded insights into what members and partners value most and suggestions to better streamline the amount of information shared, updates to the Portal, and more.

8,039 Individual Surveys Sent

13% Increase in Response Over 2021

> "The E-ISAC provides a valuable service by allowing those in the energy industry to collaborate on common concerns in the physical and cyber security space. This allows an entity to learn about and address potential threats."
>
> E-ISAC Member Organization

Feedback-Driven Changes

Member-driven feedback from the survey and other sources led to the following enhancements in 2023:

- **Streamlined Information, Direct to Members:** The E-ISAC created new products in a consolidated format such as the E-ISAC Member and Partner Weekly Shares Summary.
- **Improved Portal User Experience:** Updates on the Portal prioritized user access to the most critical information as well as improved functionality for Designated Approving Officials.
- **Introduced New Severity Rating:** The E-ISAC rolled out a new vulnerability severity rating system for prioritizing the urgency of Cyber Threat Intel Reports, Cyber Threat Hunt Reports, and other related posts.
- **Automated Information to Save Members' Time:** The E-ISAC introduced cutting-edge technology such as a new Threat Intelligence Platform (TIP) and updated real-time automated sharing feeds so information is sent in a more timely, efficient manner.

SECTION 4

A Look Ahead

In 2024, the E-ISAC's strategic priority focus areas include:

- **Provide curated security information:** Members and partners will benefit from curated actionable security intelligence and risk mitigation measures through the Portal, workshops, automated information sharing, briefings, and seminars.
- **Conduct advanced intelligence gathering:** Threat hunts will identify malicious technology on IT and OT platforms, which will be communicated to members and partners.
- **Expand CRISP:** Priorities for CRISP include: expanded participation, technology modernization, and planning for its next generation.
- **Focus on member feedback:** Expanded collection and use of member feedback will lead to improved products and services and a better user experience on the Portal.
- **Grow E-ISAC membership:** The E-ISAC will strategically expand membership by focusing on NERC registered entities, natural gas companies, and renewable energy providers, as well as growing the Vendor Affiliate Program.
- **Prioritize GridEx recommendations:** Following the release of the GridEx VII Lessons Learned report, tabletop attendees will convene to review and validate the recommendations. GridEx VIII planning will also begin.

E-ISAC and CRISP Anniversaries

This milestone will be commemorated throughout the year, including at GridSecCon 2024 on October 22-25 in Minneapolis, Minnesota.

25 YEARS

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

This year also marks CRISP's 10th anniversary.

10 YEARS

E-ISAC

CRISP

CYBERSECURITY RISK INFORMATION SHARING PROGRAM

CONTACT THE E-ISAC

Now, more than ever, the electricity industry must work together to ensure a reliable, resilient, and secure grid. Contact the E-ISAC here:

24/7 Operations Center:
operations@eisac.com

Membership Questions:
memberservices@eisac.com

Speaker Requests:
speakerrequests@eisac.com

Vendor Affiliate Program:
vendorprogram@eisac.com

CRISP:
crisp@eisac.com

Visit EISAC.com for information about the E-ISAC and to apply for membership.

**All statistics, except as noted, are for calendar year 2023.*