Information Sharing Guide

TLP:CLEAR Disclosure is not limited.

Overview

The E-ISAC serves as the electric sector's primary security information-sharing platform, enhancing the ability of its members and partners to prepare for and respond to cyber and physical security incidents, threats, and vulnerabilities. The E-ISAC gathers, analyzes, and shares security-related information to produce risk-based intelligence, identify emerging trends, deliver mitigation strategies, and provide other actionable resources. Information shared with the E-ISAC empowers situational awareness across the North American grid, strengthening industry collaboration and readiness.

Why Share?

- Enable earlier detection of emerging cyber and physical security threats
- Contribute to aggregated, data-driven analysis, informing industry and risk-based decision-making
- Exchange lessons learned, mitigations, and best practices
- Leverage E-ISAC reach-back capabilities and intelligence community partnerships
- Fortify coordinated response and collective defense of the North American power grid

What to Share?

- Cyber or physical security events and incidents
- Suspicious or anomalous activity indicating reconnaissance, targeting, or exploitation
- Impacts to corporate or operational technology environments, including actual or potential security-related outages, degraded monitoring and control capabilities, and disruptive events
- Insider-related incidents affecting security
- Indicators, trends, patterns, or forensic findings pertinent to sector-wide awareness
- Relevant law enforcement or intelligence assessments, including suspected intent or attribution

How to Share?

- Email: operations@eisac.com
- Portal: Members can post with or without attribution and set notification preferences
- Phone: The 24/7 Watch Operations Team can be reached at (202) 790-6000
- Automated exchange through E-ISAC program participation

RELIABILITY | RESILIENCE | SECURITY

TLP:CLEAR

Examples of What to Share

Cyber Security

- Relevant information focused on adversary tactics, techniques, and procedures, which may align with the MITRE ATT&CK framework
- Adversary activity that may affect corporate or operational systems, such as host and network-based indicators of compromise
- Malware identified within enterprise or operational environments
- Suspicious or anomalous network traffic within trusted environments or from partner networks
- Suspicious activity targeting remote access infrastructure (VPN, jump hosts, remote gateways, etc.) including unexplained authentication attempts or anomalous account activity
- Phishing activity or social engineering attempts
- Reconnaissance, vulnerability scanning, probing, or exploitation activity
- Forensic findings or threat hunting insights relevant to sector awareness

Physical Security

- Suspicious activity, including surveillance, video, or photography of facilities or personnel
- Impersonation or social engineering attempts targeting physical access
- Theft, loss, or diversion of essential safety or security equipment and materials
- Unauthorized or unusual UAS (drone) activity near or over facilities
- Activist activity targeting or potentially affecting facilities, operations, or personnel
- Expressed or implied threats or assaults against personnel
- Breach or attempted unauthorized entry into facilities
- Vandalism, including arson, graffiti, cut wires, or other damage to infrastructure
- Gunfire or ballistic damage to facilities or equipment
- Degradation of monitoring, control, communications, or physical security systems
- SCADA/EMS anomalies occurring in conjunction with a physical security event

"I appreciate the E-ISAC, their information, collaboration, and willingness to assist when questions arise. Information provided is intuitive, relevant, timely, and actionable. E-ISAC staff are helpful and professional."

– Scott Parker, Manager, Physical Security & Emergency Management, Snohomish PUD

Information Protection

The E-ISAC operates under a strict code of conduct that protects member-shared information and ensures separation from NERC's and the ERO Enterprise's enforcement functions.

Confidential or attributable information is not disclosed without the organization's explicit consent. Identifiable member information is removed prior to broader distribution unless explicitly approved, in accordance with established policy and TLP guidance.

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

– Electric Cooperative Leader and 2023 JD Power Survey Respondent

TLP:CLEAR

Information Sharing Programs and Services

CRISP

The Cybersecurity Risk Information Sharing Program (CRISP) is a cyber threat intelligence program strengthening the collective defense of the nation's energy sector through a unique public-private partnership between the E-ISAC and the United States Department of Energy (DOE).

Open to asset owners and operators in the electric, oil, and natural gas subsectors, as well as ancillary energy sector support organizations, this fee-based service leverages advanced technology and industry expertise to deliver timely, actionable threat intelligence related to activity observed within participant IT networks. Network data is collected through information sharing devices (ISDs) deployed in participating environments, enabling CRISP analysts to identify threat actors, detect emerging trends, and analyze cross-sector indicators.

Participants retain ownership of their data and engage directly with CRISP analysts for tailored insights, threat interpretation, and response support. CRISP's bidirectional information sharing with DOE elevates sector-wide resilience and situational awareness.

For more information, please contact crisp@eisac.com.

Best for members seeking near real-time visibility into advanced cyber threats affecting their IT environments through a DOE partnership and analyst expertise.

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

– E-ISAC Member Organization and 2023 JD Power Survey Respondent

ESSIX

The Electricity Sector Security Information eXchange (ESSIX) is the E-ISAC's automated information-sharing platform. ESSIX provides an automated STIX/TAXII feed of cyber indicators of compromise (IOCs) and E-ISAC Portal bulletins, enabling direct integration into member security platforms and threat intelligence systems. This automation reduces latency and manual processing, allowing organizations to operationalize E-ISAC intelligence more efficiently within existing security workflows. ESSIX leverages the Cyware platform to support secure, standardized information exchange.

For more information, please contact performance@eisac.com.

Best for members wanting automated ingestion of IOCs and E-ISAC bulletins into existing security tools.

TLP:CLEAR

Bulk Data Sharing

The E-ISAC Physical Security Bulk Data Sharing Program creates a trusted space for the electric industry to securely share incident data and benefit from the resulting aggregated analysis. By combining data from participating members under a unified framework, the program delivers meaningful benchmarking, trend analysis, and personalized risk assessments.

Participating members voluntarily share their physical security incident data, typically in an Excel or CSV file, on a weekly or monthly basis with the E-ISAC. In return, members receive tailored, data-driven analysis highlighting emerging patterns, comparative benchmarks, and potential areas of elevated risk. This enhanced visibility facilitates risk-based decision-making and supports more effective resource allocation.

Best for members looking for structured benchmarking and risk insights tailored to their organization's physical security footprint.

For more information, please contact physicalsecurity@eisac.com.

"The partnership that we have developed with the E-ISAC has been instrumental in how we have revamped our security posture at several critical sites. The high-level data analysis presented by the E-ISAC has proven to be highly impactful, leading to a significant reduction in incidents. We look forward to continuing this ongoing collaboration and impeccable professionalism shown by [the E-ISAC]."

– Corporate Security Intelligence Specialist and E-ISAC Bulk Data Partner

VISOR

VISOR (Vulnerability and Exposure Insight through Search and Organizational Review) delivers timely, tailored analysis of externally observable cyber vulnerabilities and exposures using benign, publicly available information from trusted open-source platforms such as Shodan and Censys. The program identifies internet-reachable systems, indicators of outdated software, insecure configurations, and other externally visible conditions that may increase cyber risk. When reporting thresholds are met, E-ISAC analysts review, validate, and enrich findings with contextual commentary, confirmation of online accessibility, and risk-informed mitigation considerations.

Best for members desiring analyst-reviewed insight into externally visible vulnerabilities and exposures affecting their organization.

VISOR reports provide structured, actionable insights that support remediation prioritization, planning, and leadership communication for CISOs, engineers, and SOC teams. Through VISOR, members decrease external exposure risk while fortifying broader sector awareness.

For more information, please contact operations@eisac.com.

Frequently Asked Questions

Q: How should I choose the appropriate method of information sharing?
A: Automated and bulk data exchange programs are effective for continuous, high-volume indicator sharing. Routine incidents, indicators, and questions are best shared via Email or the Portal. For active incidents, urgent concerns, or time-sensitive events, please call our Watch Operations Team at (202) 790-6000.

Q: What types of information should I share with the E-ISAC?
A: If activity appears suspicious, anomalous, or potentially impactful to security or operations, it is appropriate to share. Early sharing helps the E-ISAC assess potential trends and broader sector implications. When in doubt, contact Watch Operations for guidance.

Q: When sharing a cyber or physical security incident, what details are helpful to include?
A: For cyber security incidents, helpful details (when available) include host or network based indicators; observed tactics, techniques, and procedures (TTPs), such as initial access vectors, exploited vulnerabilities, or living-off-the-land activity; the date and time of events; affected assets or environments; any known or suspected threat actor information; and whether law enforcement was contacted. For physical security incidents, useful details (if known/applicable) include the type and location of the impacted asset; whether the incident resulted in an outage; suspected motivation; estimated damage or loss; and whether law enforcement has been notified.

Q: What if I only have limited or preliminary information?
A: Share what you know as early as possible, even if details are incomplete. Early notification enables the E-ISAC to identify potential trends and assess sector-wide implications. Information can be updated as additional details become available.

Q: Will sharing information trigger regulatory or enforcement action?
A: The E-ISAC maintains separation from NERC's enforcement functions and does not conduct compliance or regulatory reviews. Information shared with the E-ISAC is used to enhance situational awareness and support collective defense. Sharing information with the E-ISAC does not replace any applicable mandatory reporting requirements under NERC Reliability Standards or other regulatory obligations. Members remain responsible for fulfilling required reporting obligations to appropriate authorities.