A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP:WHITE - Disclosure is not limited.

Guide for Information Sharing

September 2019

Overview

The E-ISAC serves as the primary security communications channel for industry, and enhances the ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents. The E-ISAC gathers, analyzes, and shares security information from members and partners; coordinates incident management; enables member to member sharing; and shares mitigation strategies with interdependent sectors and government partners. Information that members share with the E-ISAC helps create an understanding about security threats that may impact the industry.

Information Protection

The E-ISAC protects member-shared information through security controls within the secure E-ISAC Portal and through procedure, policy, legal documentation, and physical and logical separation from NERC. E-ISAC policy prevents sharing of confidential or attributable information without consent of the organization that provided the information. Any confidential or attributable information is stripped from materials prior to sharing.

Examples of What You Should Share

Cyber Security

Activity that may result in enterprise or operational information access, integrity, availability or confidentiality being compromised:

- Unexplained operational technology (OT) device behavior (e.g. freezes, reboots, or failures)
- Suspicious network traffic within a trusted environment or from a trusted partner’s environment
- Suspicious interaction attempts against remote access solutions (VPN concentrators, jump boxes, remote email solutions, etc.)
- Unexplained internal or external login attempts
- Targeted phishing activity with a well-defined purpose/objective
- Vulnerability probing and exploitation activity
- Malware delivered to or found in enterprise or operational equipment
- Any other analysis, insights, and forensic artifacts from incident response and threat hunting

Physical Security

- Unusual observation, suspicious activity, or surveillance of facilities
- Misrepresentation of affiliation
- Theft, loss, or diversion of key safety or security items, systems and technologies
- UAS incidents, activities, regulations
- Activist activities
- Expressed or implied threats
- Breach or attempted intrusion
- SCADA/EMS anomalies coincident with a physical security event
- Gunfire damage or other vandalism

How to Share

- Post to the E-ISAC Portal: www.eisac.com (members can post with attribution or anonymously)
- Email operations@eisac.com
- Call the 24-hour Operations Desk: 202-790-6000