A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Electricity Information Sharing and Analysis Center

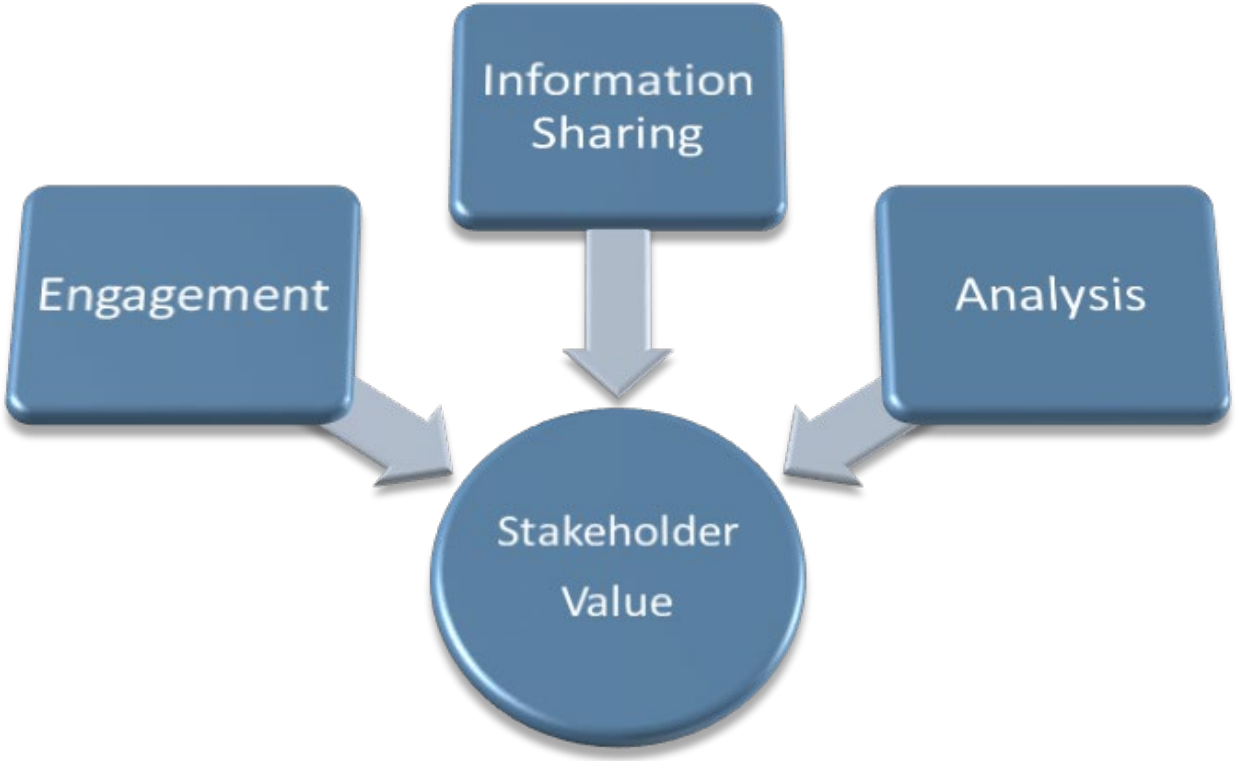
Elvin Ramirez, Senior Cyber Threat Intelligence Analyst, Cyber Intel

November 3, 2022

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

E-ISAC OVERVIEW



Protecting the North American Power Grid

E-ISAC Partners

NRECA America's Electric Cooperatives
Electricity Canada | Électricité Canada
national council of ISACs
Public Safety Canada | Sécurité publique Canada
Natural Resources Canada | Ressources naturelles Canada
Canada
ESCC Electricity Subsector Coordinating Council
JE-ISAC Japan Electricity Information Sharing and Analysis Center
EE-ISAC Information sharing in network of trust
CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
AMERICAN PUBLIC POWER ASSOCIATION
EEI Edison Electric INSTITUTE
WATER ISAC
MS-ISAC Multi-State Information Sharing & Analysis Center
SEIA Solar Energy Industries Association®
EPSA
DNG-ISAC
INGAA Interstate Natural Gas Association of America
AGA American Gas Association
ONG-ISAC Information Sharing & Analysis Center — Fueling the Exchange of Cyber Intelligence
NATIONAL GOVERNORS ASSOCIATION
Homeland Security
FS-ISAC
U.S. DEPARTMENT OF ENERGY
NARUC National Association of Regulatory Utility Commissioners
INL
Pacific Northwest NATIONAL LABORATORY
NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
NCC
Analysis & Resilience Center FOR SYSTEMIC RISK

What to Share with E-ISAC

- The E-ISAC is focused on sharing information across the North American electricity industry to reduce risk of cyber and physical security incidents.
- **Cyber Security**
  - Suspicious Traffic
  - Vulnerability probing and exploitation activity
  - Malware and Open Source reporting specific to our members
  - Analysis, insights, forensic artifacts from incident response and threat hunting
- **Physical Security**
  - Unusual observation, suspicious activity, or surveillance of facilities
  - Expressed or implied threats
  - Breach or attempted intrusion

Information Sharing Process

- **Information Sharing Channels**
  - E-ISAC Portal: www.eisac.com
  - Share Incident: operations@eisac.com
  - Phone: 202-790-6000 (24/7)

- **Info Sharing Process**
  - Assess incoming information
  - Draft Portal post; request permission to post
  - Finalize with member; post to the Portal

- **Bulk Data**
  - Can be weekly, monthly, raw data, processed data
  - Tailored to your processes
  - Critical to conducting trend analysis

E-ISAC Products and Services

- 24/7 Watch Operations
- E-ISAC Portal
  - Physical/Cyber Incident Bulletins
  - Situational Reports
  - White Papers on Emerging Issues
- E-ISAC Threat Hunt Reports
- E-ISAC Monthly Briefings
- Webinars
- Online Threat Platforms
- Risk Assessment Tools
- GridEx and GridSecCon
- Industry Engagement Program

CRISP Overview

E-ISAC CRISP
CYBERSECURITY RISK INFORMATION SHARING PROGRAM

- Public-Partnership between E-ISAC and DOE
- Near Real-Time sharing of IT network information between electricity utilities, DOE resources (PNNL), and the E-ISAC
- Bi-directional sharing of Threat Intelligence
- CRISP provides Cyber Intelligence instead of Cyber Security
- CRISP Participants gain unique insights:
  - Monitoring unusual activity within its members' networks
  - Understanding threat actor motivations and intent
  - Highlighting cyber, physical, and insider threats
  - Reporting that is actionable and informed
- CRISP is a fee-based service open to asset owner and operators in the electricity, oil, and natural gas sector

Get Involved

- E-ISAC Membership
  - All electricity industry asset owners and operators and select government partners in North America
  - Intended audience: security directors, cyber and physical security analysts, general managers
  - Those with CMEP roles may not be an E-ISAC member
- Request Membership
  - Visit www.eisac.com
- Share Info: Operations@eisac.com
- Contact Us: MemberServices@eisac.com