

A DIVISION OF NERC



E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

Electricity Information Sharing and Analysis Center

Laura Brown, Director, Programs and Engagement, E-ISAC
APPA Regional Cyber Security Summit
August 22, 2019

TLP:GREEN

RELIABILITY | RESILIENCE | SECURITY





Mission

The E-ISAC reduces cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration

Vision

To be a world-class, trusted source for quality analysis and rapid sharing of security information for the electricity industry



- Primary cyber and physical security communications channel for the electricity industry
 - Collaborates with U.S. and Canadian governments
 - Analyzes and shares voluntary security information provided by members and partners

Who can join? (Membership is free*)

- Electricity asset owners and operators, and select government and cross-sector partners
- Intended audience: security directors, cyber and physical security analysts, and general managers

Why participate?

- Customized situational awareness
- Services, events

How do you join?

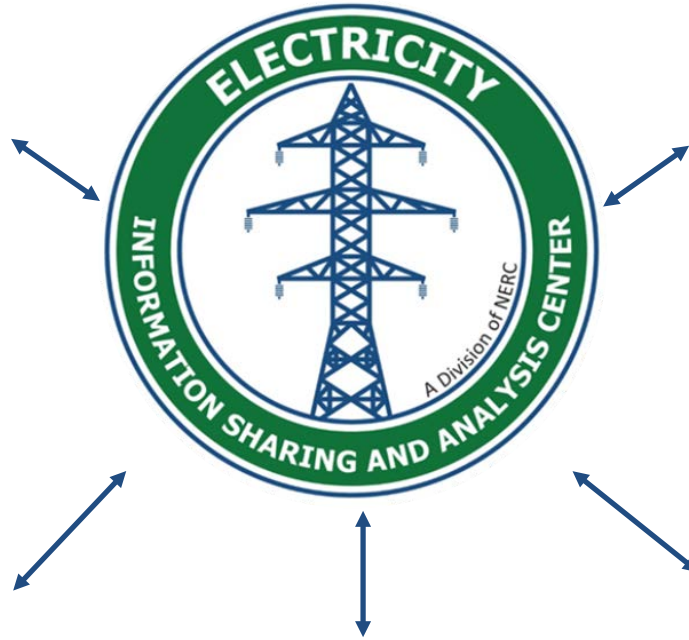
- Register at www.eisac.com



E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Partnerships



U.S. Government



Canadian Government



Trade Associations



International ISACs (Japan and European)



Other ISACs

How to Share

- Channels to share with the E-ISAC
 - Calls or emails to Watch Operations
 - Portal posts
 - Cybersecurity Risk Information Sharing Program (CRISP) reports

- E-ISAC Portal: www.eisac.com
- E-mail: operations@eisac.com
- Phone: [202-790-6000](tel:202-790-6000)

Who to Share With

- Asset owner and operator members
 - Investor-owned utilities, munis, co-ops
- Partners
 - U.S. and Canadian federal governments
 - ISAC partners
 - International partners





What to Share

- Cyber security
 - Indicators of compromise
 - Phishing emails
 - Software vulnerabilities
 - Operational technology threats
 - Tactics, techniques, procedures (TTP)
- Physical security
 - Intrusions
 - Theft
 - Gunfire
 - Unmanned Aircraft Systems/Drones
 - TTPs



Credential Harvesting



Exploitation of trusted relationships

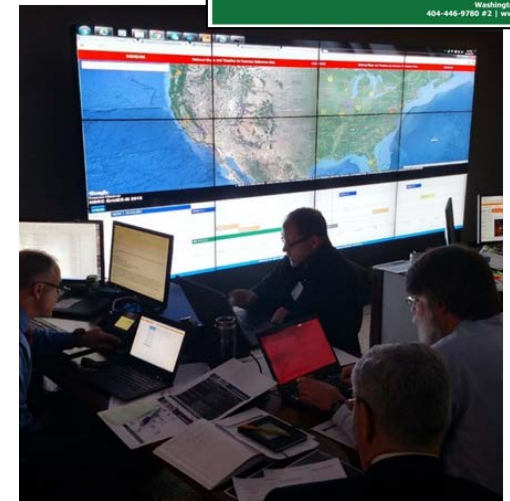
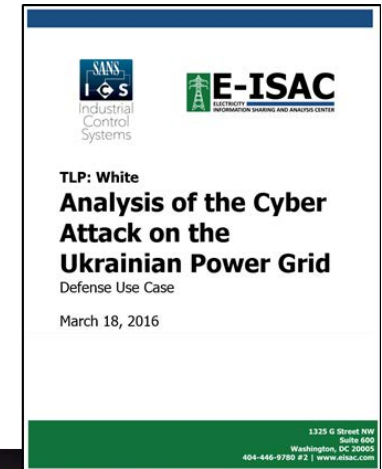


Network Device Tampering



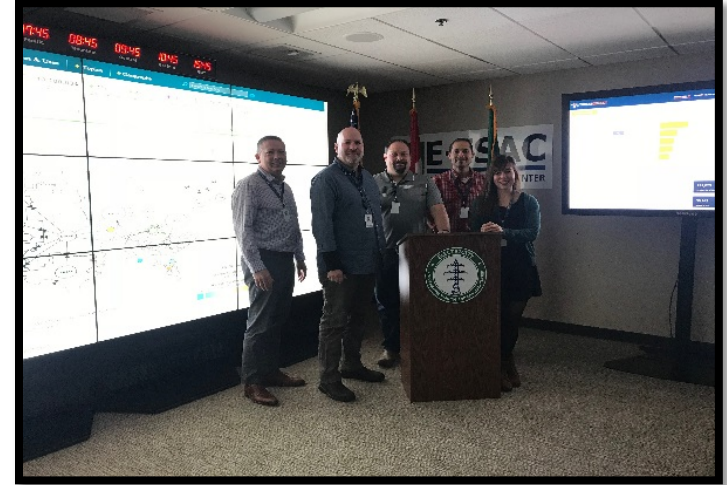
Use of Native Tools

- Products
 - Issue-specific reports
 - Incident (cyber and physical) bulletins
 - Weekly and monthly summary reports
 - NERC Alerts
- Services
 - Critical Broadcast Program (CBP)
 - Monthly briefing series
- Tools
 - E-ISAC Portal (www.eisac.com)
 - CRISP





- Programs
 - Industry Engagement Program (IEP)
 - Analyst Deep Dives (Cyber and Physical)
- Conferences and Events
 - Grid Security Conference (GridSecCon)
 - Classified and unclassified workshops
 - Grid Security Exercise (GridEx)
- Meetings
 - Visit Member Companies
 - Conduct E-ISAC Executive Tours





- IEP is a multi-day immersive learning experience for electricity industry analysts
 - Three days
 - Small classes (four people)
 - Free training
- Who can participate?
 - Electricity industry asset owner and operator organizations
 - Cyber and physical security analysts and managers
- IEP by the numbers
 - 2018-2019: 13 sessions, with 46 participants from across industry
 - 2020: Six session dates forthcoming



GRIDSEC CON 2019 NERC · SERC

- North America's premier electricity industry security conference
- October 22-25, 2019, in Atlanta, GA
- GridSecCon goals
 - Promote reliability of the grid through training and exercise
 - Deliver cutting-edge discussions on critical infrastructure threats
 - Inform industry with security best-practice discussions on reliability, mitigation, and threat awareness
- To register, please visit:
<https://web.cvent.com/event/fe28a6ff-cb87-4e16-b329-3f63c1728fdf/summary>

Day One – Training Day

- SANS 'Netwars', Physical Security, Exercise Planning, and more

Day Two – Threat Day

- Supply Chain Threat Vectors Panel
- Cyber Attacks with Physical Effects Panel
- Future Threats – What Comes Next? Panel

Day Three – Solutions Day

- Cyber Threat Intelligence Panel
- The Electricity-Natural Gas Nexus Panel
- Security Solutions Lightning Round

Day Four – Briefings and Tours

- Unclassified and classified briefings
- Security tours of critical infrastructure



- **Exercise dates: November 13-14, 2019**
- GridEx V: unclassified exercise designed to simulate a cyber/physical attack on electric and other critical infrastructures across North America
- Participants include a variety of stakeholders
- **Registration ends September 30, 2019**
 - Email GridEx_registration@bah.com to register



GridEx V
GRID SECURITY EXERCISE 2019



NERC
NORTH AMERICAN ELECTRIC
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER



- Become a Member
- Share information with the E-ISAC and interact with our analysts
- Participate in E-ISAC events
 - Monthly briefings
 - IEP
 - GridSecCon 2019
 - GridEx V



A stylized map of North America, including the United States, southern Canada, and northern Mexico. The map is rendered in shades of blue and grey. A solid blue horizontal band crosses the middle of the map, serving as a background for the title text.

Questions and Answers