A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Electricity Sector Threat Landscape

Manny Cancel, NERC Senior Vice President and E-ISAC CEO

NEPPA 2023 Annual Conference

August 22, 2023

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY

Agenda

- NERC / E-ISAC Overview
- Threat Landscape
  - Cyber
  - Physical
- E-ISAC Events
  - GridSecCon
  - Grid Ex VII
- Collective Defense

NERC Overview

- International, independent, not-for-profit organization
- Mission: To assure the effective and efficient reduction of risks to the reliability and security of the grid
- Oversees reliability and security for a bulk power system (BPS) that provides electricity to approximately 400 million people

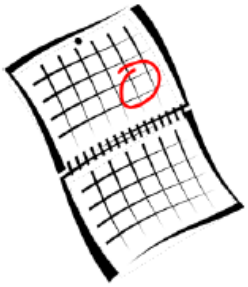
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

NERC Focus Areas

- **Energy:** Tackle grid transformation; climate change-driven, extreme weather; and inverter performance issues
- **Security:** Focus on supply chain, Information Technology (IT) and Operational Technology (OT) system monitoring, cyber-informed grid planning and design, and evolution of the Critical Infrastructure Protection (CIP) standards
- **Agility:** Be more nimble in key areas – standards development, internal operating processes, technical deliverables, revisit the FERC settlement restrictions, and explore alternate funding mechanisms
- **Sustainability:** Invest in ERO systematic controls, eliminate single points of failure, strengthen succession planning, and ensure robust cyber security protections for all systems
- **And … everything else we need to do**

Reliability History: Key Dates



1965: Northeast blackout

1968: National Electric Reliability Council (NERC) established by the electric industry

1996: August 10th WSCC blackout; worst in the West

2002: NERC operating policy and planning standards become mandatory and enforceable in Ontario, Canada

2003: August 14th blackout; worst to date

2005: EPAct Section 215 Federal Power Act creates the Electric Reliability Organization (ERO)

2006: Federal Energy Regulatory Commission (FERC) certifies NERC as the ERO; Memorandums of Understanding (MOUs) with some Canadian Provinces

2007: North American Electric Reliability Council becomes the North American Electric Reliability Corporation (still NERC); FERC issues Order 693 approving 83 of 107 proposed reliability standards; reliability standards become mandatory and enforceable

E-ISAC History

- 1998 – President issues Presidential Decision Directive (PDD)-63, calling for a national effort to assure the security of the nation's critical infrastructure
  - PDD-63 leads to formation of sector-specific information sharing and analysis centers (ISACs)
- 1999 – U.S. DOE endorses NERC to operate the E-ISAC

E-ISAC Membership

- Membership
  - ~1,800 members - electricity industry asset owners and operators and select government partners in North America
  - 44% of NEPPA utilities are E-ISAC members
  - Intended audience: security directors, cyber and physical security analysts, general managers
  - Compliance Monitoring and Enforcement Program personnel may not be an E-ISAC member
  - Membership is no additional cost
  - Members receive customized situational awareness on:
    - Security Threats
    - Cyber and Physical Bulletins
    - Critical Broadcast Program Alerts

E-ISAC Partners

A DIVISION OF NERC

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

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

AMERICAN PUBLIC POWER ASSOCIATION

EEI
Edison Electric INSTITUTE

EE-ISAC
Information sharing in network of trust

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

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

NATIONAL GOVERNORS ASSOCIATION

ONG-ISAC
Information Sharing & Analysis Center
Fueling the Exchange of Cyber Intelligence

Homeland Security

NARUC
National Association of Regulatory Utility Commissioners

FS-ISAC

U.S. DEPARTMENT OF ENERGY

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NCC

Analysis & Resilience Center
FOR SYSTEMIC RISK

INL

Pacific Northwest
NATIONAL LABORATORY

TLP:CLEAR

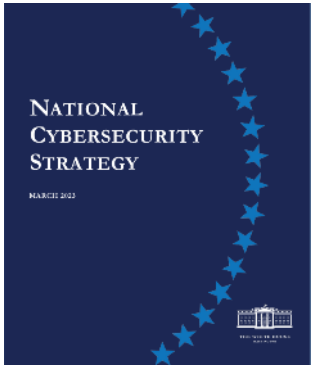
Threat Landscape

*Not a question of **if**, but **when**… focus on mitigations*

- Capable adversaries, especially: China, ransomware actors, and insider threats (cyber and physical)
- Unprecedented number of hardware/software vulnerabilities
- Supply chain risk resulting from third party compromises
- Increase in physical security incidents
- Potential risk from drones

Cyber Strategy

- U.S. Office of the Director of National Intelligence (ODNI) Annual Threat Assessment
- Canadian Centre for Cybersecurity Threat Assessment
- U.S. National Cybersecurity Strategy



Nation-State Adversaries

Nation states possess the capability to disrupt critical infrastructure in North America and continue to target the electricity sector

- Russia – a top cyber threat employing espionage, influence, and attack capabilities
- China – one of the most dynamic cyber threats demonstrating increasing sophistication and adaptive techniques
- Iran – a major threat with growing expertise and willingness to conduct aggressive cyber operations
- North Korea – cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat

Cyber Threats

- **China**
  - Volt Typhoon targeting U.S. utility and other critical infrastructure sectors
  - Storm-0558 hacks U.S. Commerce and State Departments
  - Continued exploitation of MS Cloud, Citrix, Fortinet, VMware, Log4j vulnerabilities
  - Improved tradecraft and evasion techniques
- **MOVEit File Transfer Supply Chain Compromise**
  - Cl0p ransomware gang extortion campaign
  - U.S. Government and Service Providers impacted
- **Prominent Vulnerabilities**
  - Barracuda Email Security Gateway replacement advisory
  - Fortinet Fortigate SSL-VPN
  - Rockwell Automation ControlLogix Communication Module

Ransomware

- Frequent activity from multiple groups — no customer outages
- Executes high impact attacks, extort funds, disrupt services, and expose data
- Releases captured data and encryption
- Targets virtual machine hosts, network storage, and ICS
- Supply Chain Victims
  - Engineering firms
  - Construction companies
  - Equipment manufacturers

Cyber Supply Chain Threats

- Global supply chain challenges (materials and transportation)
- Probe of Rockwell Automation by U.S. government
  - Security concerns on software facility located in Dalian, China developing code
  - Potential vulnerabilities that allow Chinese state actor access to U.S. critical infrastructure systems
  - E-ISAC monitoring Rockwell devices exposed on internet
- Compromise and data breaches of key vendors
  - Hitachi and ABB
  - Sargent & Lundy, Black & McDonald
  - Dragos

Cyber Response/Resources

- **Services**
  - Analytic collaboration with ETAC and cross sector ISACs
  - Threat hunting in CRISP data
  - Monitoring of Dark Web, criminal forums, social media
  - Outreach to members with vulnerable devices on internet
  - E-ISAC Cl0p MOVEit victim list
  - Separate monthly briefings for members and regulatory partners
- **Products**
  - All-Points Bulletins (Volt Typhoon, IBM Maximo)
  - Critical ICS and IT vulnerabilities reports
  - Cyber Threat Intelligence reports with mitigations
  - Monthly ICS threat and trends report
  - Weekly ransomware report
  - Weekly Small and Medium Utility Community reports

Cyber Mutual Assistance

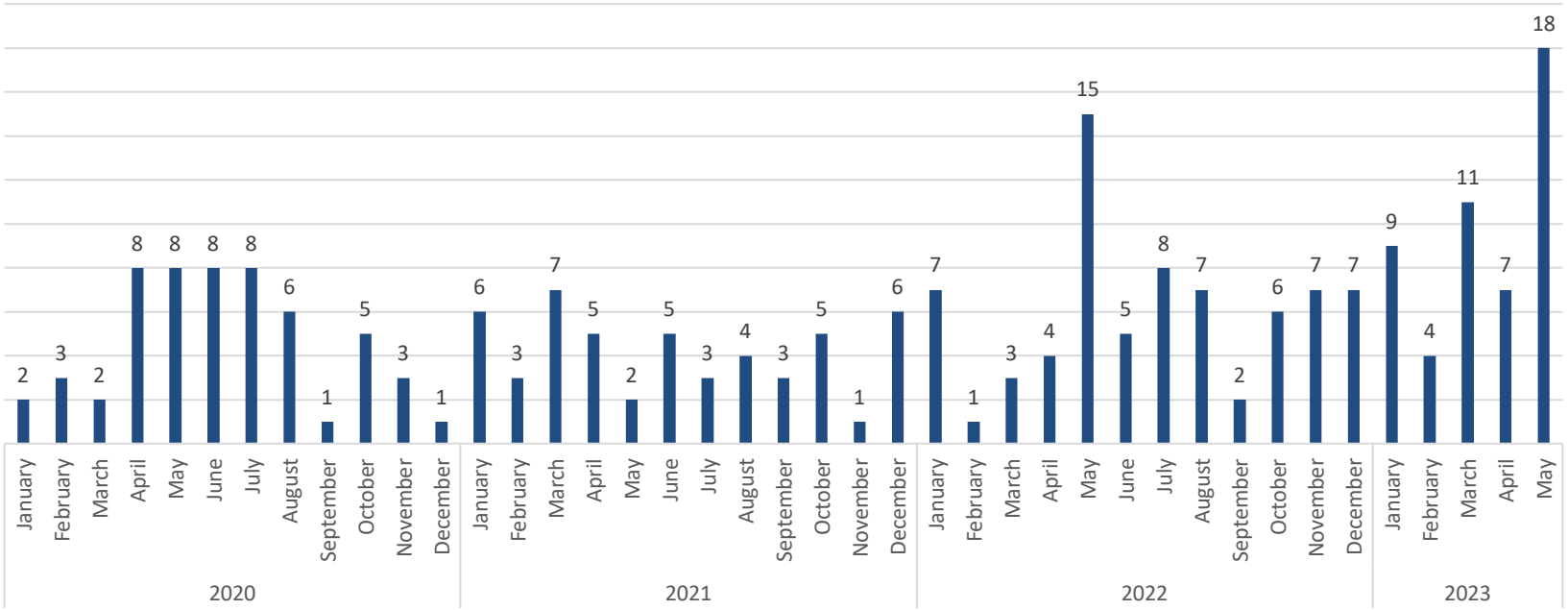
- CMA Program: includes industry cyber experts who can provide **voluntary assistance** to each other in advance of, or in the event of, a disruption of electric or natural gas service, systems, and/or IT infrastructure due to a cyber emergency
- **Participation:**
  - Over 180 participating entities in the U.S. and Canada (Investor-owned, Public Power, Cooperatives, RTOs/ISOs)
  - Covers more than **90%** of U.S. electricity customers, **85%** of U.S. domestic natural gas customers, **1.25 million** electricity customers in Canada
- It is intended to be **advisory and short-term** and may include **services, personnel, and/or equipment**

Physical Threats

- 2020-2022: E-ISAC Physical Security Report: Grid-Impacting Incidents (2020-2022)
  - Of the physical security incidents shared with E-ISAC between 2020-2022, 97% resulted in no grid impact and 3% resulted in outages or other grid impacts
  - Notable increase in Q3-4 2022 compared to baseline trends over the previous 18 months
- 2023 Observations (thus far): E-ISAC Physical Security Quarterly Report, Q1 2023
  - Overall, the number of grid impacting (Level 2/3) incidents have decreased from Q4 2022, but are still elevated compared to historical numbers
  - Level 2/3 incidents in 2023 have involved similar types of tactics as seen in Q4 2022: vandalism, intrusion (tampering), ballistic damage, and theft

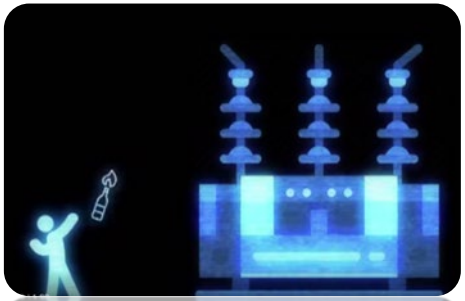
Ballistic Damage Incidents

- Continue to trend in elevated numbers in 2023 compared to historical incidents
- Most concerning tactics include ballistic targeting of substation transformers and switches (most likely to cause outages and heavy damages)
- Most common assets targeted include transmission assets (e.g., conductors, insulators, and structures) followed by substations (e.g., power transformers, voltage control equipment, and circuit breakers)



Number of Ballistic Damage Incidents Shared Monthly Since 2020

Emerging Threats Against the Grid

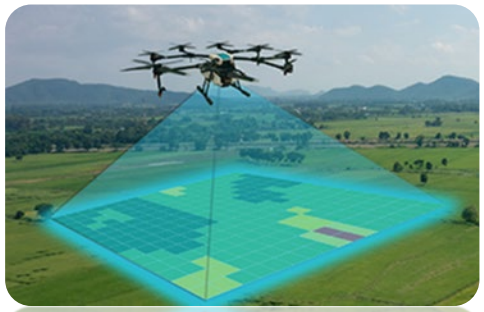


Domestic Violent Extremists

DVEs continue to utilize online platforms to frequently promote and circulate physical attack tactics against electricity assets.

Insider Threats

Insider threats within the electric industry pose a serious risk against the electric industry with the opportunity to result in result in sensitive data breaches, reputational damage or operational impact.



Drones

With the rapid technological expansion of drones, utilities faces new risks and threats posed by both malicious and non malicious drone users.

E-ISAC Response

- Regular engagement with members, partners, and stakeholders
  - Intelligence community classified briefings
  - Cross-sector collaboration
  - Threat assessments
  - Joint tri-sealed products (JCAT First Responder's Toolbox: Electric Power Substation Terrorist Threat Awareness, Detection, and Initial Post-attack Response Consideration)
- E-ISAC mitigation tools and resources
  - Physical Security Resource and Risk Management Guide
  - Identifying Possible Avenues of Approach and Firing Positions at Substations
  - Online Threat Monitoring Report
  - Drone Detection Pilot
  - White Papers (UAS, Copper Theft, and Wind Farm Security)
  - Design Basis Threat and VISA Workshops, road show

Physical Security Workshops

Workshop Overview:

- Cost-effective methodology
- Relies on subject matter expert input to determine overall system effectiveness
- Promotes developing sound business case to make informed risk-based decisions
- Provides confidence that a threat can be mitigated
- Helps utilities produce a portfolio of scenarios to justify upgrades
- View VISA workshop promotional video here

VISA stats:

- 18 workshops since 2017
- 7 workshops in 2023
- 75% increase in number of workshops held from 2022 to 2023

What's next:

- Identify options to support increased demand over next 5 years

GRIDSECCON 2023

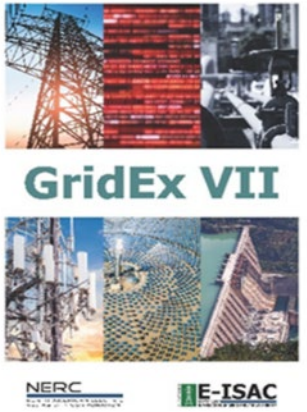
NERC • E-ISAC • NPCC

- Registration is open
- Two hotel options: Hilton Québec City Hotel and Delta Québec
- General Sessions, Keynotes, and Panels
- 10 training sessions and 24 breakout sessions
- For more information or sponsorship inquiries, please contact events@eisac.com

GridEx

- Distributed Play (E-ISAC members and partners), November 14–15, 2023
  - Audience: E-ISAC members and partners, to include electricity industry, government agencies, other relevant organizations
  - Goal: exercise emergency response and recovery plans in response to simulated cyber and physical security attacks and other contingencies affecting North America's electricity system

- Executive Tabletop (invitation only), November 16, 2023
  - Audience: industry and government executives from the ESCC, EGCC, and impacted entities
  - Goal: highlight the extraordinary operational measures necessary in response to severe combined cyber and physical attacks



Collective Defense Actions and Considerations

- **Share with E-ISAC and government/law enforcement**
  - Connect to E-ISAC and government automated sharing
  - Ensure compliance organization facilitates not hinders sharing
- **Deploy Internal Network Security Monitoring (INSM)**
  - Deploy INSM in critical OT networks and share data and analytics
- **Focus on physical security mitigation strategies and the Electricity Sector Design Basis Threat**
- **Ensure cyber security informs supply chain procurement, operations, and contract language**
  - Ensure disconnection plans in place if a vendor is compromised
  - Ensure compromise disclosure requirements embedded in contract language
  - Ensure new renewable generation is secure by design

Questions and Answers

CRISP Overview

- SUGGEST REMOVING
- Network sensing, big data processing, analysis, and information sharing – cyber intelligence vs. cyber security
  - Enables and manages the near real time sharing of IT network information
  - Leverage access to high value government threat information through DOE resources to provide data enrichment
- Participants **own** their data
- Community benefits
  - ArmorText
  - CRISP workshops
  - Governance structure