

A DIVISION OF NERC



# E-ISAC

ELECTRICITY  
INFORMATION SHARING AND ANALYSIS CENTER

# Opportunities Through Information Sharing and Analysis Centers

Frank Honkus, Associate Director of Intelligence and CRISP Manager  
October 29, 2020



**USAID**  
FROM THE AMERICAN PEOPLE



TLP:GREEN – Limited disclosure, restricted to participants **RELIABILITY | RESILIENCE | SECURITY**





- Electricity Information Sharing and Analysis Center (E-ISAC)
  - Information Sharing, Partnerships, and Analysis
- Cybersecurity Risk Information Sharing Program (CRISP)
  - Public Private Partnerships: “Being the Strongest Link”





- The E-ISAC serves as a cyber and physical communications channel for the electricity industry
  - Collaborate with U.S. and Canadian industry members, government, and cross-sector partners
  - Gather, analyze, and share voluntary information provided by members and partners
  - Information shared within the E-ISAC is protected from regulatory enforcement



- Cyber and Physical Information
- Originator control (Traffic Light Protocol (TLP))
  
- Information Sharing Channels
  - E-ISAC Website: [www.eisac.com](http://www.eisac.com)
  - E-mail: [memberservices@eisac.com](mailto:memberservices@eisac.com)
  - 24/7 Watch







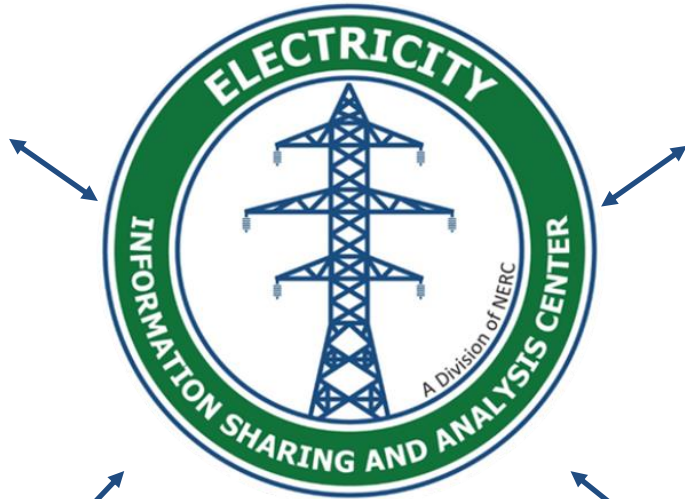
U.S. Government



National Council of ISACs



Other ISACs



International ISACs (Japan and European)



Canadian Electricity Association

Association canadienne de l'électricité

Trade Associations



Public Safety Canada

Sécurité publique Canada



CANADIAN CENTRE FOR CYBER SECURITY

CENTRE CANADIEN DE CYBERSÉCURITÉ



Natural Resources Canada

Ressources naturelles Canada

Canadian Government



- Membership Eligibility

- 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 regulatory roles may not be an E-ISAC member

- Benefits

- Membership is no additional cost
- Members receive customized situational awareness on:
  - Security Threats
  - Cyber and Physical Bulletins
  - Critical Broadcast Program Alerts



- CRISP (Cybersecurity Risk Information Sharing Program)
- Public-private partnership with government
  - Leverage government information to provide data enrichment
- Roles and responsibilities: E-ISAC and a national laboratory





- CRISP is network sensing, big data processing, analysis, and information sharing
- CRISP provides
  - Understating threat actor motivations and intent
  - Illuminate cyber, physical, and insider threats
  - Provide actionable and informed reporting



- Products

- Nation state and non-nation state threat assessments
  - Weekly and biweekly cyber activity snapshots
- Indicators associated with identified threat actors and anomalies
- Trend analysis and participant-wide analytics



- Goal: To be the strongest link for high level security situational awareness so as to protect utilities, the grid, and the nation from malicious cyber actors
- Unique collaboration between government and private industry makes CRISP the only near real-time network data-sharing program of its kind
- Provides invaluable context to help participants identify a path forward to help mitigate threats against critical infrastructure

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