FERC

Office of Energy Infrastructure Security

Craig Barrett
Office of Energy Infrastructure Security
Federal Energy Regulatory Commission
July 25, 2018

Disclaimer

The views expressed herein are the presenter's and do not necessarily reflect the views of the Commission, individual Commissioners, Commission staff, or individual Commission staff members.

Office of Energy Infrastructure Security (OEIS) Overview

Mission

OEIS provides leadership, expertise and assistance to the Commission to identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber and physical attacks.

Background

- OEIS is the newest office at FERC
- Created in late 2012 in response to growing cyber and physical security threats to energy infrastructure
- Through collaborative and voluntary programs, OEIS works with jurisdictional entities to:
  - share threat information,
  - analyze vulnerabilities and risk, and
  - help develop advanced mitigation strategies.
- OEIS is not responsible for promulgating mandatory standards or conducting enforcement actions
- OEIS is committed to identifying and sharing best practices to help improve the cyber and physical security of the bulk power system.

Focus

- Developing recommendations for identifying, communicating and mitigating potential cyber and physical security threats and vulnerabilities including Geomagnetic Disturbances (GMD) and Electromagnetic Pulses (EMP)
- Providing assistance, expertise and advice in identifying, communicating and mitigating potential cyber and physical threats and vulnerabilities
- Participating in collaborative efforts related to cyber and physical security matters
- Conducting outreach with private sector owners, users and operators of energy delivery systems regarding identification, communication and mitigation of cyber and physical threats

Activities

- Identify vulnerabilities and threats to critical energy infrastructure;
- Inform federal partners, states, key stakeholders and other strategic partners of security threats and vulnerabilities;
- Conduct proactive and reactive security assessments in collaboration with federal partners to convey threat and vulnerability information to industry including:
  - Electric utilities,
  - Oil and natural gas pipelines,
  - Hydropower, and
  - LNG facilities;
- Address threats and vulnerabilities by developing, and encouraging the adoption of best practices.

Resources

- OEIS has specialized engineering analysis capabilities to:
  - Perform power system modeling and event analysis
  - Review natural gas interdependencies and collaborate with ISO/RTOs to determine impacts
  - Work collaboratively with federal partners on the development of a strategic infrastructure policy and plans
  - Perform physical security reviews of energy facilities with federal partners

Resources (Continued)

- OEIS has specialized Cyber Security capabilities to:
  - Perform cyber architectural reviews
  - Perform state-of-the-art IT/OT network log analysis with other federal partners at DHS ICS-CERT, Idaho National Labs (INL), and Kansas Intelligence Fusion Center (KIFC)
  - Assist State Commissions in developing guidelines for evaluating cyber security plans
  - Analyze and disseminate security threat information and mitigation strategies
  - Review NERC E-ISAC Alerts and Industry Advisories

Questions?