# Rail Electrification Council of NEMA

October 20, 2021

# Overview

CYBERSECURITY

PHYSICAL SECURITY

- **Worldwide Threat Assessment of US Intelligence Community April 2021**
  - https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

- **Department of Defense, Defense Science Board, Task Force on Cyber Deterrence, February 2017**
  - https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf

- **DHS Binding Operational Directive 17-01, September 2017**
  - https://cyber.dhs.gov/bod/17-01/

# Recent Cybersecurity Events

SolarWinds Supply Chain Compromise

Microsoft Exchange Server Vulnerabilities

Ivanti Pulse Secure & Nobelium

Colonial Pipeline Ransomware Attack

Blackberry QNX Vulnerability

# FERC Two-Pronged Approach

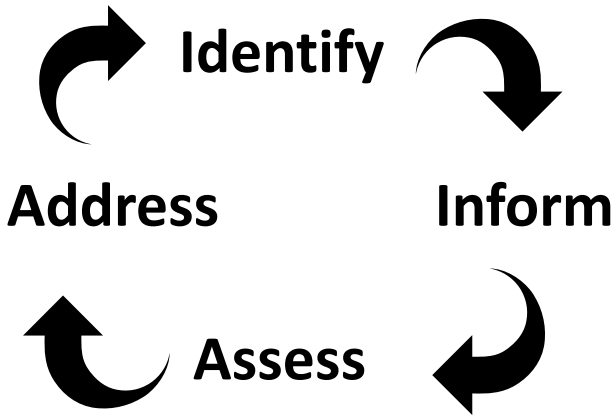
1. Establish Broad Foundational ***Regulations through NERC***

2. Identify and Promote voluntary ***Best Practices*** to Address Advanced and Targeted Threats to Key Facilities

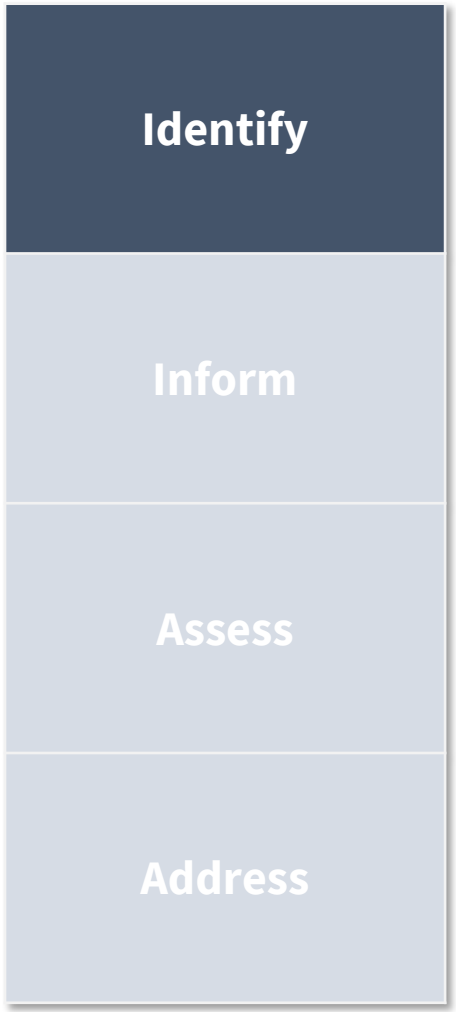
# Collaborative Questions that Produce Protective Actions

## *Security-Focused Discussions:*

1. **Do you know who's targeting your systems and how?**
2. **Do you know how to stop them?**
3. **Have you identified the systems that are most critical?**

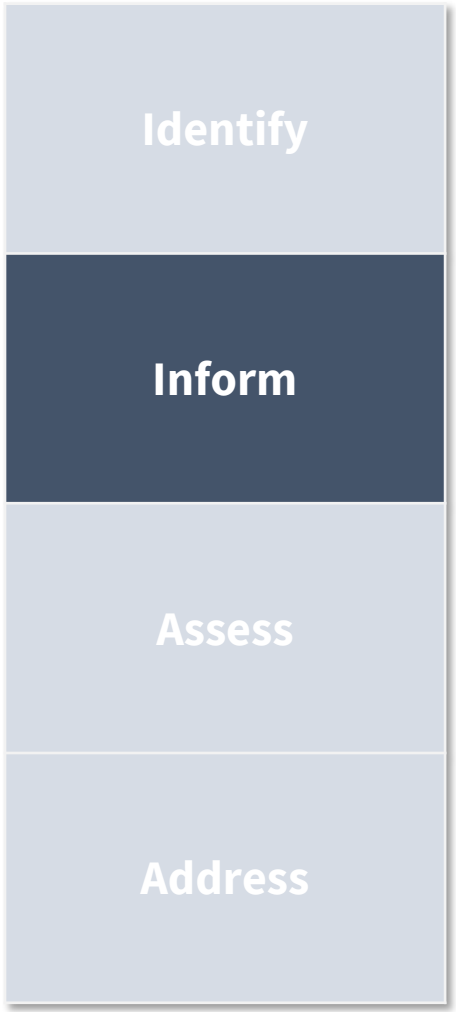


# OEIS Initiatives - Identify



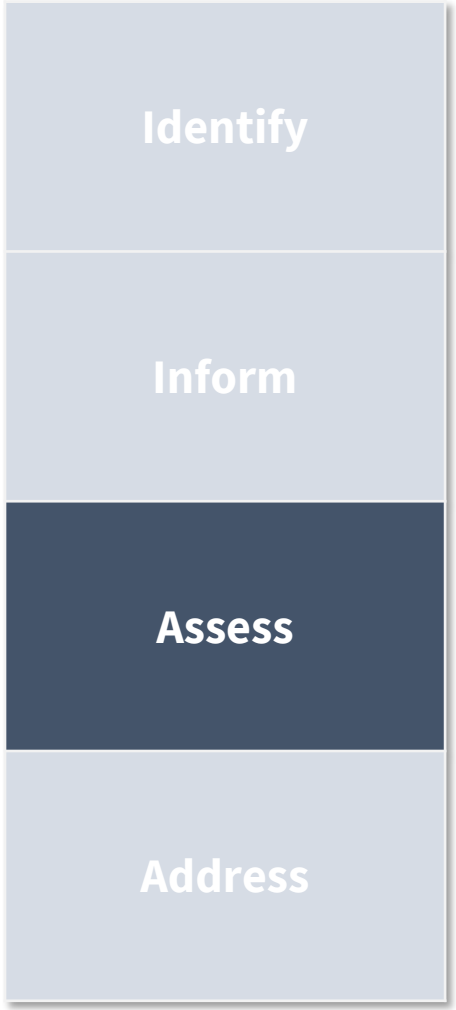

- OEIS employees are **DHS PCII certified** and are participants in the **DHS CISA Integrated Operations Coordination Center (CIOCC) or CISA Central** collaborating with federal, state, and private sector subject matter experts on threats to energy infrastructure and best practices to stop them.
- OEIS staff regularly participates in interagency meetings and with DOE, DHS, the **National Security Council** and others
- OEIS **is assisting DOE** with several cyber and physical security initiatives to identify processes and systems critical to protect the BPS against**; supply chain threats**, **EMP events**, and the effects of the **COVID-19 pandemic**.
- OEIS is assisting **DOE and DOD** with determining how owners/operators of **defense critical electric infrastructure (DCEI)** can increase security and resilience to better protect the power grid from advanced threats.

# OEIS Initiatives - Inform



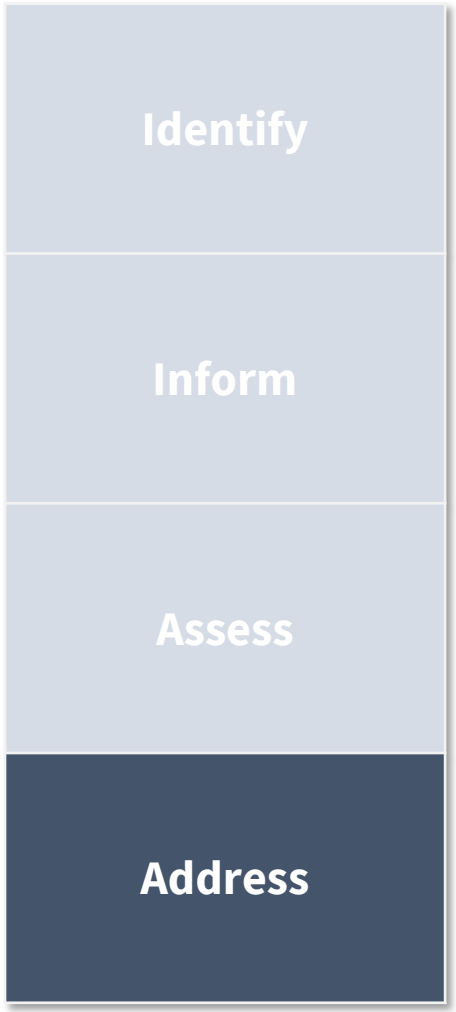

- OEIS partners with **ODNI** to facilitate **analytic exchanges** to the energy sector and state commissions using a **1-day** security clearance.
- OEIS works with **NERC and the E-ISAC** to develop, and review **alerts** and **analyses** that NERC issues to the energy sector to enable them to quickly address new vulnerabilities and threats.
- Where possible OEIS **works broadly** to inform industry of threats and mitigations; for example, OEIS has released whitepapers and provided webinars (e.g., **Cloud Security Whitepape**r with the NATF and subsequent webinar, a **whitepaper on SolarWinds with NERC,** Insider Threat Webinar).
- OEIS developed a **cybersecurity 101** training program for **state regulators**; presenting it to **45** states, **DC** and **PR** at **four** separate regional conferences and participated in the **DC Cybersecurity Technical Conference** in April, 2020.
- OEIS **is a nominating authority** for the DHS Private Sector Clearance Program; helping FERC jurisdictional energy infrastructure owners/operators to be informed of relevant **classified** threat information.

# OEIS Initiatives - Assess




- Since 2012, OEIS has conducted **dozens of IT/OT Network Architecture Assessments and physical security reviews** for electric, ONG pipeline (TSA), hydroelectric, and LNG facilities (USCG) jurisdictional to FERC.
- OEIS assists with the planning, preparation, and organization of several **cyber and physical security tabletop exercises** such as: **Cyber Yankee** which pairs NE National Guard units with utilities to simulate cyber attack and defense, **NERC's GridEx** which simulates nationwide cyber and physical attacks on utility systems, and the interagency **FEMA-led National EMP Exercise** which assess federal capabilities, roles, and responses to an EMP affecting energy infrastructure.

# OEIS Initiatives - Address




- OEIS developed a **State Regulator's Checklist**, **Cybersecurity Incident Response List**, and **IT Program Policy Guide** to assist both the states and industry to better secure energy infrastructure.
- OEIS is an **active participant** assisting with the draft of **API STD1164 2nd Edition cybersecurity standards** and **the DHS ICTSCRM Task Force** to develop **premier ICT supply chain strategies** ultimately better protecting energy infrastructure.
- OEIS **assisted TSA with its SD2 regulations** to address cybersecurity on pipelines.
- OEIS is the lead office for FERC on **key COVID-19 activities** assisting our jurisdictional utilities to assure energy service during the pandemic; developed a **joint FERC/DOE/NATF/NERC pandemic plan** for industry use; working with DOE/DHS on **official guidance** to recognize **energy workers and services as essential** assisting with **worksite access**, employee **COVID testing**, and **PPE**; participating in the **ESCC** to proactively **identify and address** threats to energy service, and participating with FERC program offices to **develop FERC initiatives** to assist industry (e.g., **policy statement**, regulatory **relief**, technical **conference**, etc.)