MOSAICS
2020 INDUSTRY DAY

Agenda

1. Bio
2. What is the E-ISAC?
3. Nation state OT cyber threat
4. Nation state case study
5. Need for MOSAICS-like capabilities

MOSAICS
2020 INDUSTRY DAY

Bio

- Frank Honkus – E-ISAC Associate Director of Intelligence Program and CRISP Manager

- Experience:
  - DOE IN: CRISP data analysis and cyber threat
  - USCYBERCOM: Red team lead and foundational author of the mitigation and recovery sections of the JBASICS ACI-TTP
  - USCYBERCOM J2: Cyber threat analysis focusing on OT/ICS/SCADA
  - DHS: supported banking and finance, telecoms, and IT sectors

Unclassified Distribution A

MOSAICS
2020 INDUSTRY DAY

What is the E-ISAC?

- The E-ISAC serves as a cyber and physical communications channel for the electricity industry
  - Collaborates with U.S. and Canadian industry members, government, and cross-sector partners
  - Gathers, analyzes, and shares voluntary information provided by members and partners
  - Information shared within the E-ISAC is protected from regulatory enforcement
- Cybersecurity Risk Information Sharing Program (CRISP)
  - Private-public partnership between DOE and electricity sector
  - Leverages government information to provide data enrichment

MOSAICS
2020
INDUSTRY
DAY

Nation State OT Cyber Threat

ODNI Worldwide Threat Assessment

Russia:
"Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."

China:
"China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."

MOSAICS
2020
INDUSTRY
DAY

A need for MOSAICS-like capabilities

- Technologies like MOSAICS enable OT:
  - Visualization
  - Virtualization
  - Analysis
  - Detection
  - Mitigation
  - Recovery

- Use case: CRISP
- The threat is real and is not going away
- Holding OT environments held at risk equals holding the nation hostage