Panel IV: Addressing the Evolving Cybersecurity Threat

Presentations: There is a widespread understanding among policymakers and industry that cyberattacks are a persistent and growing threat to the reliable or resilient operation of the Bulk-Power System. This panel will shed light on opportunities to collaboratively address existing and emerging cyber threats and vulnerabilities. Examples of recently publicized cyberattacks against industrial control systems include compromises of vendor systems and the cyber supply chain, and increasingly destructive malware. Additionally, vulnerabilities have been revealed in the structure of the processors underlying most cyber systems themselves. Panelists will be asked to address the following:

How are current trends in cyber threats and vulnerabilities affecting the behavior of grid owners and operators? How can grid operators be better prepared to protect their systems from these threats? How do you recommend organizations mitigate cyber risks?

Answer: Four things that organizations can do to mitigate Cyber risks are: 1) Enhance IT cyber situational awareness with Operational Technology (OT) and Physical Security (cameras, physical access control systems) data, establish OT/IT SOCs staffed with IT and OT SMEs; 2) Evolve from Cyber security to Cyber resilience per NIST SP 800-160 Volume II; 3) Attend and participate in information sharing groups such as the Electricity ISAC; 4) Provide continual training and table tops/exercises for their OT/IT Security SMEs.

How can the Critical Infrastructure Protection Reliability Standards (CIP Standards) be improved to assist responsible entities in addressing emerging cyber threats?

A: By changing in two ways: 1) Evolving from Cyber security to Cyber Physical System (CPS) resiliency; 2) Addressing Cyber and operational risks from deployed Distributed Energy Resources (DER) and Energy IoT devices.

What information-sharing practices are required? How are best practices developed, applied, and improved? How could other technologies be deployed securely to help manage the emerging grid?

A: Other technologies that could be deployed to help manage the emerging grid are smart decentralized phasor measurement unit (PMU)-based control systems that would react autonomously in real-time to prevent and/or self-heal Grid disturbances or anomalies.

The Commission engages with other agencies and industry in mitigating the risk posed by cyber threats – including promoting information sharing,

identifying and assessing threats, sharing lessons learned and best practices. How can we improve these efforts?

A: By better resourcing and supporting FERC's voluntary organization, the Office of Energy Infrastructure Security, they could work in voluntary partnership with the private sector, DOE, and DHS.

How can cyber incident response plans be improved to address the evolving cyber threat landscape? For example, when a cyber system is compromised, anti-malware software may not identify the system as compromised, and the only indicator may be the system's abnormal behavior.

A. Cyber incident response plans can be improved by adopting a Continuous Diagnostics and Monitoring (CDM) approach, to include monitoring with supporting analytics based on Techniques Tactics and Procedures (TTP) or adversary behavior to identify the root cause of incidents. Identification of the critical data from the OT networks and devices and the analytics can be shared across the sector.

When considering the emerging cyber threats to industrial control systems, what strengths and weaknesses in the body of CIP Reliability Standards are revealed? What role can the voluntary development, application, and sharing of best practices play?

A: No comment.