Testimony of Joseph McClelland
Director, Office of Energy Infrastructure Security
Federal Energy Regulatory Commission
Before the Committee on Oversight and Reform
Subcommittee on National Security
United States House of Representatives
July 27, 2021

Testimony

Chairman Lynch, Ranking Member Grothman and Members of the Subcommittee:

Thank you for the privilege to appear before you today to discuss potential threats to the bulk power system in the United States. My name is Joe McClelland, and I am the Director of the Office of Energy Infrastructure Security at the Federal Energy Regulatory Commission (Commission). I come before you as a Commission staff witness, but I should note that my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

I'd like to begin today by briefly describing the Commission's work regarding the reliability and security of the bulk power system. I'll then describe the Commission's two-pronged approach to these issues. This approach includes, first, our role in establishing and enforcing mandatory reliability standards, which are administered by the Commission's Office of Electric Reliability. The second prong of the Commission's approach is our role in addressing advanced, persistent threats with best practices and mitigation mechanisms by partnering with other federal agencies, the states and the industry on a collaborative basis. The Commission's Office of Energy Infrastructure Security, or OEIS, is charged with oversight of this second prong.

In the Energy Policy Act of 2005 (EPAct 2005) -- specifically through section 215 of the Federal Power Act (FPA) -- Congress entrusted the Commission to approve and enforce mandatory reliability standards for the nation's bulk power system. Section 215 requires the Commission to certify an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the nation's bulk power system. The Commission certified the North American Electric Reliability Corporation (NERC) as the ERO. By statute, the bulk power system does not include electric distribution facilities.

The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States only after Commission approval.

The Commission may approve newly proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification to address a specific matter but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

Section 215 of the Federal Power Act provides for stakeholder input in the ERO's development of reliability standards for the bulk power system. Consistent with the FPA, NERC uses an accredited process, approved by the American National Standards Institute, which is intended to develop consensus among stakeholders on both the need for, and the substance of, a proposed standard. This process works relatively well to develop standards to address "traditional" operations and planning-related reliability events that may cause grid failures or blackouts, such as improper vegetation management or failures associated with the operation of protection equipment.

The nature of the national security threats by adversaries intent on attacking our nation's electric grid significantly differ from the reliability vulnerabilities that have caused regional blackouts and reliability failures we faced in the past. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens. These threats originate from a variety of new and quickly emerging sources, such as from supply chain compromises, insider attacks, targeted phishing attempts, ransomware campaigns, internet-of-things vulnerabilities, and many more.

To help mitigate these advanced, persistent, and rapidly-evolving threats, the Commission uses a two-pronged approach with regard to grid reliability: employing mandatory reliability standards to establish foundational practices while also working collaboratively with industry, the states and other federal agencies to identify and promote best practices.

For instance, regarding mandatory reliability standards, the Commission has approved Critical Infrastructure Protection, or "CIP" Reliability Standards, to establish a baseline to address critical and fundamental matters, including security management controls, protection of removable media, patch management,

personnel training, and cyber incident reporting. These Reliability Standards are updated over time to address emerging issues. As one example, the Commission modified the CIP Reliability Standards in 2018 to help address supply chain risk management for cyber assets. The supply chain risk management standards went into effect on October 1, 2020.

While the NERC CIP Reliability Standards are the foundation of the Commission's work to address cybersecurity, there are additional measures that can and should be taken to improve industry's cybersecurity posture in light of these rapidly evolving threats. That is why the Commission established OEIS.

OEIS partners with other federal agencies, states, and industry to develop and promote best practices for critical energy infrastructure security. Working with these entities, OEIS helps identify new and emerging threats, inform the private sector of them, performs voluntary cybersecurity evaluations, and assists with mitigating actions.

For example, OEIS conducts voluntary architecture assessments of interested Commission-jurisdictional utilities' computer networks that control the operations of their facilities. Conducted onsite, these assessments are specific to the organization, reviewing everything from the configuration of legacy equipment to the application of state-of-the-art protection systems.

Another example is that OEIS works with the Office of Director of National Intelligence, specifically the National Counterintelligence and Security Center, to conduct briefings and exchange information with state and industry officials about the current threats industry is facing and what can be done to address them. More broadly, OEIS works with the NERC Electricity Information Sharing and Analysis Center to rapidly issue bulletins and alerts, informing industry of specific vulnerabilities and threats as well as best practices that can defend against them. In fact, OEIS worked with the NERC Electricity Information Sharing and Analysis Center (E-ISAC) to issue an industry-wide white paper explaining supply chain compromises such as SolarWinds and what actions can be taken to protect against them. This document was released on July 7, 2021. This was an effort by FERC and NERC to ensure we are continuing to communicate with the electric power industry on the need for continued vigilance on cyber matters. The report highlights lessons learned from recent supply chain compromises and encourages the industry, including entities that did not install SolarWinds on their networks, to take all recommended actions that the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) outlined to help protect the bulk power system.

As a final example, OEIS assists with the planning and execution of table-top exercises and participates in joint security programs with other government

agencies. Last month OEIS assisted the National Guard units and participating utilities in the New England states to conduct Cyber Yankee, a simulated cyber-attack on utility system networks. This red-teaming exercise helped the utilities and National Guard units to prepare for these threats, including practicing government assistance to the utilities as part of defense and recovery efforts. Exercises such as this are critical to maintaining readiness and ensuring our ability to respond to cybersecurity events.

In conclusion, cybersecurity threats pose a serious risk to the bulk power system and its supporting infrastructures that serve our nation. These are complex, persistent, and fast-evolving issues. They won't be solved easily, and they require a great deal of coordination and communication. Therefore, the Commission has adopted this two-pronged approach to best address the important security matters, including collaboration with our federal, state, and industry partners.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.