Testimony of Michael A. Bardee
Director, Office of Electric Reliability
Federal Energy Regulatory Commission
Before the Subcommittee on Energy
Committee on Energy and Natural Resources
United States Senate
March 28, 2017

Introduction

Chairman Gardner, Ranking Member Manchin, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Michael Bardee. I am the Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

The Commission's role on reliability is to help protect and improve the reliability of the Nation's Bulk-Power System through effective regulatory oversight as established in the Energy Policy Act of 2005 (EPAct 2005). My testimony summarizes the Commission's oversight of the reliability of the Bulk-Power System and, specifically, the Commission's implementation of that authority with respect to cybersecurity. I then address S. 79, the Securing Energy Infrastructure Act.

FERC's Reliability Authority

In EPAct 2005, Congress tasked the Commission with a responsibility to oversee mandatory, enforceable reliability standards for the Nation's Bulk-Power System (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 applies only to the Bulk-Power System, not facilities used in local distribution.

Section 215 requires the Commission to select an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards to help protect and improve the reliability of the Nation's Bulk-Power System. The Commission certified as the ERO the North American Electric Reliability Corporation (NERC). 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 ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval.

The Commission may approve proposed reliability standards or modifications to the 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 on a specific matter but it does not have the authority to modify or author a standard.

FERC and Cybersecurity

Cybersecurity is an important part of the Commission's responsibility to oversee reliability standards for the Bulk-Power System. In 2006, NERC proposed to the Commission an initial set of cybersecurity standards, known as the Critical Infrastructure Protection (CIP) standards. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "bulk electric system." In 2008, the Commission approved NERC's proposed CIP reliability standards while also directing NERC to develop modifications. Since then, the Commission has approved various changes to the CIP standards. The CIP standards specify mandatory requirements for utilities, including: how to identify and categorize cyber assets and systems; processes and procedures for maintaining these systems; and ensuring that only appropriate personnel have access to these systems, among others. Last year, utilities implemented version 5 of the CIP standards for high- and medium-impact assets. This year, utilities are implementing version 5 for low-impact assets.

In July 2016, the Commission directed NERC to develop a reliability standard addressing the supply chain for industrial control system hardware, software, and related services associated with the bulk electric system. Specifically, FERC directed NERC to develop an objective-based standard that would require each affected utility to develop and implement a plan that includes security controls for its cyber supply chain. FERC ruled that the standard should address four areas: ensuring that the software used to run these systems is authentic; ensuring that remote access by vendors to these systems is secure; information system planning; and vendor risk management and procurement controls. There is no requirement for any specific controls, nor does FERC require any "one-size-fits-all" requirements. Instead, FERC said that the standard should require utilities to develop a plan to meet the four objectives, while allowing flexibility on how to meet the objectives. NERC is working on a standard now, and is due to submit it to the Commission in September 2017.

Also in July 2016, FERC issued a Notice of Inquiry (NOI) on whether to modify the CIP standards regarding the cyber protection of control centers used to monitor and control the Bulk-Power System. FERC cited the 2015 cyberattack on the electric grid in

Ukraine as an example of how cyber systems used to operate and maintain interconnected networks more efficiently can have the unintended effect of creating cyber vulnerabilities. FERC sought comment on possible changes to the CIP standards to address separation from the Internet and to require a computer practice for preventing unauthorized programs from running, known as "application whitelisting." FERC is reviewing the comments submitted in response to the NOI, and considering whether further action is appropriate on these issues.

While mandatory standards are an important component of the Commission's work on cybersecurity, FERC also works with industry in other ways to enhance security. For example, FERC's Office of Energy Infrastructure Security (OEIS) provides leadership, expertise, and assistance in identifying, communicating, and seeking comprehensive solutions to significant potential cyber and physical security risks to the energy infrastructure under the Commission's jurisdiction. OEIS works directly with governmental and private sector energy industry entities to identify and share information on threats and vulnerabilities, and to promote voluntary mitigation practices that are complementary to mandatory regulations promulgated and enforced by the Commission and by state authorities. Engaging with the regulated community outside of the traditional regulatory process facilitates the necessary exchange of timely information and subsequent implementation of state-of-the-art protective measures.

The goal of the Commission's CIP standards and other cyber-related efforts is to mitigate the risk of a cyber incident that harms the reliability of the electric grid. However, in case such an event ever happens, utilities also need to be prepared to restore and recover the Bulk-Power System. For this reason, in January 2016, FERC completed a report with NERC and its Regional Entities on restoration and recovery of the grid. The joint review by FERC and NERC staff gathered information from a sample of utilities, and found they have extensive incident response and recovery plans. The report recommended various practices, such as verifying and testing modifications to a system restoration plan, obtaining insight from utilities that have experienced widespread outages, and obtaining independent technical review of recovery plans. The report also recommended certain follow-up studies, such as how to prepare for a loss of Supervisory Control and Data Acquisition (SCADA) computers and other data sources. Work on the additional studies is ongoing.

Other Efforts

Other agencies and organizations also contribute to the reliability and security of the electric grid. The Department of Energy, for example, is the Sector-Specific Agency for electrical infrastructure. In that role, DOE works with industry, state and local agencies, and other stakeholders to help protect our electric grid. This work may take the form of research performed by the various national laboratories, as proposed in S. 79.

Other examples are the Cybersecurity Risk Information Sharing Program (CRISP) and the Electricity Subsector Cybersecurity Capability Maturity Model (C2M2).

Similarly, security is addressed by the Electricity Subsector Coordinating Council, a public/private partnership for CEOs of critical infrastructure owners and operators to engage directly with senior government officials on policy-level security issues. This includes not only FERC and DOE, but also the Department of Homeland Security, the Federal Bureau of Investigation and others.

A secure electric grid is vital to our Nation. There is no "silver bullet" that can protect the grid. Instead, it depends on the efforts of many organizations and individuals, and requires ongoing adaptation, innovation and vigilance. And it requires ongoing dialogue and cooperation, to ensure that our efforts are not at cross-purposes or inefficient.

S. 79

S. 79, the Securing Energy Infrastructure Act, would establish a pilot program to study cyber vulnerabilities and consider solutions for isolating and protecting industrial control systems. Participation in the study would be voluntary, and would include a diverse working group. The program would involve researching, developing, testing, and implementing technology platforms and standards, "to isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities." The effort would include research on analog and non-digital control systems; purpose-built control systems; and physical controls. The bill would authorize an appropriation of $10 million for the pilot program and $1.5 million for the related report and other work.

The effort proposed in S. 79 could potentially aid the utility industry, FERC and others to maintain a secure electric grid. Utilities have come to rely increasingly on digital tools for monitoring and operating the Bulk-Power System. These tools have enhanced the efficiency and effectiveness of utility operations significantly. A broad-scale reversion to pre-digital technology is uneconomic, unjustified, and perhaps even impossible. But I do not see S. 79 as proposing such action. Instead, S. 79 focuses on "the most critical systems of the covered entities." More importantly, S. 79 does not require adoption of any particular technology, and instead requires research and testing to determine if certain tools and technologies, when applied to limited circumstances, can enhance the security of the most critical systems. If this program succeeds in identifying more secure approaches for the most critical systems, the implementation of these approaches could be justified, depending on factors such as effects on operational efficiency. Over time, these approaches, if successful, also could be incorporated into new designs for an evolving Bulk-Power System. However, any decision on implementation should be made only after sufficient research and testing. These

approaches also may be useful not only in the context of the Bulk-Power System but in other industrial control systems too.

I would suggest one small change to S. 79. The working group required by S. 79 would specifically include the Department of Energy, the Nuclear Regulatory Commission, NERC and several other organizations, but not explicitly FERC. I believe FERC should also be listed as a member in the working group.

Conclusion

FERC will continue to work with the utility industry to seek ways to maintain and enhance the security of the electric grid. While mandatory reliability standards are an appropriate tool at times in this effort, other approaches are also important. S. 79 can support the goal of grid security by seeking unusual ways to reduce our risk without unduly sacrificing efficiency.

Thank you for allowing me to testify today. I would be glad to address any questions you may have.