Testimony of J. Andrew Dodge, Sr., P.E

Director, Office of Electric Reliability, Federal Energy Regulatory Commission

Before the Subcommittee on Energy

United States House of Representatives

July 12, 2019

Introduction

Chairman Rush, Ranking Member Upton, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Andy Dodge. 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.

Today, my testimony will provide a brief overview of the Commission's authorities and activities to oversee and improve the cybersecurity of the nation's bulk-power system. Our work includes mandatory reliability standards, audits of those standards, and best practices to ensure that utilities keep apace of threats. We work closely with the North American Electric Reliability Corporation (NERC), its regional entities, other Federal and state agencies, and responsible entities to carry out this important work.

FERC's Authority to Oversee Reliability

In the Energy Policy Act of 2005, Congress gave the Commission the authority to oversee the development and enforcement of mandatory reliability standards for the Bulk-Power System. The authority pertains to the interconnected electricity system (the "grid") in the United States, and excludes Alaska, Hawaii, and local distribution systems.

Section 215 of the Federal Power Act requires FERC to designate an Electric Reliability Organization (ERO) to develop, with industry, standards to ensure reliable and secure operation of the grid, which it proposes to the Commission for approval. NERC is the Commission-certified ERO. After review and approval by the Commission, compliance with the reliability standards is mandatory by users, owners and operators of the grid in the United States. NERC and its six regional entities enforce the standards and may impose penalties for noncompliance, after notice and opportunity for hearing, subject to review and approval by the Commission. The Commission may also enforce reliability standards independently of NERC.

Importantly, the ERO is responsible for developing and proposing new or modified reliability standards to the Commission. The Commission may approve new or modified reliability standards if it finds them to be "just, reasonable, not unduly discriminatory or preferential, and in the public interest." If a proposed standard does not meet this test, section 215 requires the Commission to remand it to the ERO for revision. The Commission may not write or modify a reliability standard. If the Commission determines that there is a need for a new or modified

standard, it may, on its own motion or upon complaint, direct the ERO to develop and submit a standard to meet the identified reliability need.

The Critical Infrastructure Protection (CIP) Reliability Standards

Under section 215 of the Federal Power Act, a reliability standard may include requirements related to cybersecurity protection. The Commission exercises authority in this area by overseeing NERC's development and enforcement of Critical Infrastructure Protection (CIP) reliability standards. In June 2006, NERC proposed eight mandatory critical infrastructure protection reliability standards to replace the earlier voluntary cybersecurity standards. On January 18, 2008 pursuant to section 215 of the Federal Power Act, the Commission issued Order No. 706 approving the eight CIP reliability standards, which after allowing a period of time for entities to achieve compliance. The standards became enforceable in 2010. These were the so-called "version 1" of the CIP standards and they were the first and only mandatory cybersecurity standards covering critical infrastructure. In addition, the Commission directed NERC to develop modifications to the CIP reliability standards to address specific concerns identified in Order No. 706.

Since 2008, NERC has periodically modified the CIP reliability standards, submitting new "versions" of the standards for Commission approval. Notably, in January 2013, NERC filed version 5 of the CIP reliability standards, which proposed to alter the method of identifying and protecting cyber systems by categorizing each grid-related cyber system as having a low, medium, or high impact on the reliable operations. Each of the three categories requires security provisions proportional to the specified category. The Commission approved CIP version 5 on November 21, 2013, in Order No. 791. Now, rather than referring to specific versions of the standards, we simply refer to them as the CIP standards. There are currently 11 active cybersecurity standards and one active physical security standard.

The CIP standards, viewed as a whole, are a portfolio of requirements that constitute a defense-in-depth approach to cybersecurity based on an assessment of risk. Importantly, the CIP reliability standards are objective-based and responsible entities are free to choose compliance approaches best tailored to their systems. The foundational standard (CIP-002) requires a utility to perform a risk assessment of its assets and to categorize them in terms of low, medium and high impact to the grid. Medium and high impact systems include large control centers, ultra-high voltage transmission lines, large substations and generating facilities. Most requirements apply to the high and medium impact systems. Lower impact systems include the remainder of cyber systems that are not captured in the other two categories. Other CIP standards require utilities to: develop and implement cybersecurity plans; train personnel adequately; establish physical and electronic access perimeters; test and apply patches in a timely manner; identify and report cybersecurity incidents; and develop and implement recovery plans; among others.

The CIP reliability standards continue to be reviewed and updated to address new cybersecurity challenges and technological changes. For example, the Commission recently has taken two additional important actions to further enhance the CIP reliability standards. In October 2018, FERC approved NERC's proposed reliability standards to address supply chain threats. This

action is particularly significant given that these specific threats to the energy sector continue to grow. Second, last month, at the June 2019 Commission Meeting, FERC approved a modification to a CIP standard to expand reporting requirements of cybersecurity incidents for critical grid cyber systems. Today, entities are required to report successful cyber intrusions that compromise one or more reliability tasks. The revised standard requires utilities to report both successful and attempted cyber intrusions into critical systems to NERC's Electricity Information Sharing and Analysis Center, as well as to the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). Requiring entities to report attempted cyber intrusions, as well as successful ones, is an important step toward enhancing the collection and distribution of information on rapidly evolving cyber threats.

FERC Audits the Compliance of Entities with the CIP Reliability Standards

As the ERO, NERC and its regional entities are the primary enforcement authorities for the CIP standards, and carry out a compliance program, which includes audits of utilities' compliance with the CIP standards. Starting in 2016, the Commission has been auditing a sample of utilities with respect to their CIP compliance. The audits assessed compliance with version 5 of the CIP reliability standards, which became effective on July 1, 2016. In particular, the Commission focused on utilities for whom compliance with CIP would be new, or for whom the nature of their CIP programs would have to change significantly given the risk-based approach of version 5. NERC and the relevant region participate in the audits with Commission staff.

Because the CIP standards do not prescribe how entities should comply to achieve the stated objective of a given CIP standard or requirement, there are a range of approaches that utilities implement based on the particular configuration of their electrical and computer systems. In the course of performing the audits, our staff, working with NERC and regional entity staff, observe both best practices for CIP implementation and also ways in which entities could improve their security posture and avoid issues of non-compliance. In October 2017 and again in March 2019, the Commission issued a report that describes the lessons learned from the audits, including insights into the cybersecurity and CIP compliance issues encountered by the audited entities. By publishing publicly these lessons learned we hope to help other utilities improve their compliance with the CIP reliability standards, as well as their overall cybersecurity. These lessons include:

- Making sure that a utility's security processes are well-documented and followed;
- Ensuring that cyber systems connected to generators and shared facilities are included in their risk assessments;
- Ensuring that contractors employ appropriate practices for vetting staff;
- Clearly mapping physical and electronic access rights to control rooms and electronic access systems;
- Ensuring that cybersecurity events are completely and accurately logged;
- Implementing procedures to detect and investigate unauthorized changes to cyber systems; and

- Replacing or upgrading "End-of-Life" system components, which can pose significant vulnerabilities.

FERC Works with Agencies and Utilities to Keep Abreast of Threats and Promote Best Practices

Ensuring security of the grid requires more than CIP standards compliance, especially in such a dynamic area as cybersecurity. Implementing effective cybersecurity requires a well thought-out, documented, and disciplined cybersecurity program that aligns with the mission of the organization. This means putting structure around how organizations align IT (and cybersecurity) strategy with business strategy, ensuring that they stay on track to achieve their strategies and goals, and implementing repeatable measures for their cybersecurity performance. Therefore, the Commission has adopted a two-prong approach to address threats to energy infrastructure: mandatory reliability standards overseen by our Office of Electric Reliability, and voluntary initiatives overseen by our Office of Energy Infrastructure Security (OEIS). OEIS engages with partners in industry, states, and other federal agencies to develop and promote best practices for critical infrastructure security. These initiatives include, among other things, voluntary architecture assessments of interested entities, classified briefings for state and industry officials, and joint security programs with other government agencies and industry.

Because the responsibility for securing critical infrastructure is shared across industry, federal, and state governments, the Commission continues to work collaboratively in this area. For example, on March 28, 2019 the Commission hosted a joint technical conference with the Department of Energy to discuss investments for cyber and physical security with federal, state and industry experts. The conference explored current threats against energy infrastructure, best practices for mitigation, current incentives for investing in physical and cybersecurity protections, and cost recovery practices at the state and federal level.

OEIS works closely with other agencies, including the Department of Energy, the NCCIC, the DHS National Risk Management Center, the Transportation Security Administration, the National Security Council, and others to ensure that the Commission understands evolving cybersecurity threats to FERC-jurisdictional infrastructure and that best practices in ensuring cybersecurity are identified and disseminated.

Conclusion

In conclusion, protecting the electric system from cyber and physical threats is critically important to securing our nation's critical infrastructure. The Commission is taking both a standards (mandatory) and a collaborative (voluntary) approach to ensuring the reliable and secure operation of the grid. I thank the Committee for the opportunity to participate in this hearing and look forward to answering your questions.