Testimony of Neil Chatterjee
Chairman, Federal Energy Regulatory Commission
Before the Committee on Energy and Natural Resources
United States Senate
February 14, 2019

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee:

Thank you for inviting me to appear before you today to discuss the important issue of cybersecurity in the energy sector. I appreciate the Committee's attention to this crucial issue and the role that the Federal Energy Regulatory Commission (FERC) plays in securing our nation's critical infrastructure.

I'd like to take this opportunity to highlight three major issues for the Committee: first, the evolution of mandatory reliability standards; second, the voluntary partnerships FERC has established with industry and other agencies; and third, the interdependency of the electric and natural gas systems.

Mandatory Reliability Standards

Under Section 215 of the Federal Power Act, the Commission has authority to approve mandatory reliability standards developed by the North American Electric Reliability Corporation (NERC). Once approved by the Commission, the standards are mandatory and enforceable either by NERC or independently by the Commission. The Commission also has the authority to direct that NERC develop a mandatory standard to address reliability concerns identified by the Commission. NERC's standards for cybersecurity, known as the Critical Infrastructure Protection (CIP) standards, became mandatory and enforceable in 2009.

Since then, the CIP standards have matured considerably and now form an effective framework for protections against cyber threats. The maturation of the CIP standards regime has reduced the need for constant revisions to address discrete issues and, instead, has allowed both FERC and NERC to focus on tackling emerging threats. In particular, I'd like to call the Committee's attention to two important actions that the Commission has recently taken on this front. First, at our October 2018 Commission Meeting, 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, at our July 2018 Commission Meeting, FERC approved a final rule directing NERC to expand reporting requirements for critical systems. That final rule directed NERC to develop a standard that requires registered entities to report successful and attempted intrusions into critical systems to NERC's Electricity Information Sharing and Analysis Center, as well as to the Department of Homeland Security (DHS). I believe this final rule represents an important step toward enhancing the collection and distribution of information on rapidly evolving threats.

Voluntary Partnerships

While the NERC CIP standards form an important baseline for cybersecurity practices,

compliance alone is not enough to achieve cybersecurity excellence. 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, I believe it's imperative that we continue to strengthen these partnerships. To this end, the Commission continues to work collaboratively in this area and will be hosting a joint technical conference on March 28, 2019 with the Department of Energy, state, and industry officials, to discuss investments for cyber and physical security. The conference will explore current threats against energy infrastructure, best practices for mitigation, current incentives for investing in physical and cybersecurity protections, and cost recovery practices at both the state and federal level.

I'd also like to take a moment to highlight OEIS's joint efforts with the DHS National Risk Management Center and the Transportation Security Administration (TSA) to develop better approaches for managing cybersecurity risks to natural gas pipelines. As I discuss further below, I believe securing our natural gas infrastructure is critical to safeguarding the reliability of the electric system.

Interdependency of Electric and Natural Gas Systems

As I discussed in a joint op-ed with my colleague Commissioner Glick last year, I am concerned that, because of our nation's growing use of natural gas for power generation, a successful cyber-attack on the natural gas pipeline system could have a significant impact on the electric grid. Given this increasing vulnerability, Commissioner Glick and I expressed our view that more must be done to ensure robust oversight for natural gas pipeline cybersecurity. Since the publication of that op-ed, I've been pleased to hear from many members of the natural gas pipeline community who have expressed their appreciation for these concerns and willingness to continue taking steps to improve their security posture. In addition, I recently met with TSA Administrator David Pekoske to discuss pipeline cybersecurity and was impressed by his focus on this vital issue as well as his pledge to taking further action to improve TSA's oversight of pipeline security. While I think both industry and government have made significant strides toward addressing this issue, I believe more work still needs to be done, and the Commission stands ready to assist in these efforts.

Conclusion

Protecting the energy sector from cyber threats will require each of us to do our part, and I assure you that we at the Commission are ready and willing to continue working together with each of you on the Committee, the full Congress and other agencies to bolster our nation's cybersecurity posture. Again, I appreciate the opportunity to come before you today, and I look forward to continuing this essential dialogue.