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

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

Thank you for inviting me to appear before you today to discuss 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.

Turning first to the topic of Mandatory Reliability Standards: As part of the Energy Policy Act of 2005, Congress gave the Commission authority to approve and enforce mandatory reliability standards for the nation's bulk power system, including for cybersecurity. As I'm sure Jim Robb will discuss in greater detail, EPAct '05 established a joint responsibility between the Commission and NERC, as the designated Electric Reliability Organization, for developing and enforcing the reliability standards. Because of the unique relationship between our organizations, maintaining an open and collaborative relationship between NERC and the Commission has been a top priority during my tenure. I'd like to thank Jim and the rest of the team at NERC for their dedicated efforts and I look forward to continuing our important work together.

NERC's standards for cybersecurity, known as the Critical Infrastructure Protection or CIP, standards, became mandatory and enforceable in 2009.

Since 2009, the CIP standards have matured considerably and now form an effective framework for protections against cyber threats. The evolution of these standards 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 Commission meeting last October, FERC approved reliability standards to address supply chain threats. By exploiting vulnerabilities in the electric utility supply chain, adversaries can seize on a variety of opportunities to compromise critical systems. While supply chain vulnerabilities are some of the most important to address, they're also some of the most difficult to mitigate. This is because today's utilities rely on a highly integrated global supply chain to meet their business needs. Leveraging this modern network of vendors can provide utilities with significant benefits, but it also presents difficulties in comprehensively identifying risks. While there is no silver bullet to mitigate supply chain risks, I believe this standard is a significant step in the right direction.

Second, at our meeting last July, the Commission approved a final rule directing NERC to expand reporting requirements for critical systems. That rule directed NERC to develop a standard requiring registered entities to report both 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. This final rule represents another important step toward mitigating risks by enhancing the collection and distribution of information on rapidly evolving threats.

While the NERC CIP standards form an important baseline for cybersecurity practices, compliance alone is not enough to achieve cybersecurity excellence. That's why 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, also known as 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, classified briefings for state and industry officials, and joint security programs with other government agencies and the private sector.

Because the responsibility for securing critical infrastructure is shared across the public and private sector, I'm a strong supporter of our efforts to continue strengthening these partnerships. As part of that objective, the Commission continues to work collaboratively in this area and will be hosting a joint technical conference on March 28 with the Department of Energy to discuss investments for cyber and physical security. The conference will explore current threats against energy infrastructure, best practices for mitigation, incentives for investing in physical and cybersecurity protections, and cost recovery practices at both the state and federal level.

And there's one final area where I believe continued partnership across industry and government will be essential. Because of our nation's growing use of natural gas for power generation, I'm increasingly concerned about the security of our natural gas pipeline system. Last year I joined my colleague Commissioner Rich Glick in an op-ed detailing how a successful cyber-attack on the system could have a significant impact on the electric grid. Given this vulnerability, Commissioner Glick and 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 a willingness to continue taking steps to improve their security posture. I also recently met with TSA Administrator David Pekoske and was impressed by his focus on this vital issue as well as his pledge to further improve TSA's oversight of pipeline security. While I think both industry and government have made significant strides, I believe more work still needs to be done. The Commission stands ready to assist in these efforts wherever we can.

Now before I conclude my opening statement, I want to thank each of you, again, for your efforts in this space and your time to engage in this conversation today. These are complex issues, and they won't be solved easily, but I appreciate the opportunity to come before you today and look forward to continuing this essential dialogue.