Testimony of Acting Principal Deputy Assistant Secretary Puesh Kumar, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy Before the United States House of Representatives Committee on Oversight and Reform, Subcommittee on National Security

July 27, 2021

Introduction

Chairman Lynch, Ranking Member Grothman, and distinguished members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Energy (DOE) on the Administration's continuing efforts to secure the Nation's electric grid and ensure Americans can rely on a resilient, secure, and clean energy system. My testimony today will focus on the current cybersecurity threat landscape of the United States energy sector and the important role DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) plays in addressing cyber threats.

The energy sector provides the power that all other U.S. critical infrastructure sectors depend on to operate. A disruption in the energy system can have a devastating impact to national security, the U.S. economy, and the livelihoods of millions of Americans.

CESER is focused on securing the Nation's energy infrastructure against all hazards, reducing the risks and impacts of cyber and other disruptive events, and supporting states and industry with response and restoration when a disruption occurs. These responsibilities stem from DOE's role as the Energy Sector Risk Management Agency (SRMA) and the primary agency for coordinating energy sector emergency support as Emergency Support Function-12 (ESF-12) under the National Response Framework.

Understanding Current Cyber Threats

The U.S. electric grid is becoming increasingly complex and interdependent as a result of technology innovation and greater connectivity. These rapid changes are changing the risk posture for the energy sector, creating a multi-threat environment. Cyber threats remain one of the most significant strategic risks for the United States. We have seen an increase in the frequency and sophistication of attacks by a range of actors, including hackers, cyber criminals, and nation-states.

In May 2021, the Colonial Pipeline Company proactively shut down its pipeline systems for five days after a cyber-criminal group hacked the company's information technology (IT) network using ransomware. This incident served as a reminder of the threat our cyber adversaries pose and their ability to paralyze entire states and regions through a singular cyber-attack.

Last year, the SolarWinds cyber-attack brought software supply chain cyber-attacks to our national consciousness. The sophisticated attack by the Russian Foreign Intelligence Service (SVR) compromised a software update, which then exposed as many as 16,000 computer networks worldwide. This incident highlighted the importance of securing not only the network of critical infrastructure owners and operators, but also their suppliers and manufacturers. If a similar attack vector had been used in the operational technology or industrial control systems that run energy systems, the impact could have been devastating.

While significant cyber incidents present a challenge for energy systems, they also present an opportunity. As we undergo a transformational change to a clean electric grid, we have the opportunity to design systems securely from the ground-up and apply principles such as security by design and zero trust architecture to ensure they are resilient and secure.

Electric Grid Cybersecurity Roles and Responsibilities

DOE is the Sector Specific Agency for the energy sector pursuant to the Fixing America's Surface Transportation Act (FAST Act), the SRMA for the energy sector pursuant to the 2002 Homeland Security Act (as amended), primary agency for energy sector emergency response coordination as ESF-12 per the National Response Framework, and has authorities under Presidential Policy Directive (PPD)-21 and PPD-41.

Within DOE, CESER executes those responsibilities in close coordination with other offices across the Department and with our interagency partners, including the Cybersecurity and Infrastructure Agency (CISA), Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), and other elements of the Intelligence Community.

CESER is built upon a foundation of partnerships with industry; state, local, tribal, and territorial (SLTT) communities; regulators like the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC); suppliers and manufacturers; and academia. We firmly believe that it will take all of us coming together, each with our own authorities, capabilities, and backgrounds, to address the complex cyber threats facing the energy sector. *Collective preparedness* and *collective response* are at the heart of our work.

CESER's Priorities

CESER is focused on addressing the growing landscape of threats to the energy sector, technology development, and energy system trends. I have outlined five priorities that will enable the office to execute its mission to protect our Nation's energy infrastructure from all threats and hazards.

- The first priority is to increase the visibility of cyber threats targeting energy companies' industrial controls systems. This includes giving government and industry the ability to detect and deter cyber threats through the recently announced Industrial Control Systems Cybersecurity Initiative and Electricity Subsector 100-Day Action Plan, and through training and exercises.

- The second is to identify supply chain threats and disclose vulnerabilities in energy sector systems and digital supply chain.
- The third priority is to encourage the concept of "security by design." This will ensure that cybersecurity is built into relevant research, development, and demonstration (RD&D) across DOE and the National Laboratories.
- The fourth priority is energy security capacity building in the industry and state, local, tribal, and territorial (SLTT) community. This includes strengthening threat information sharing, planning for energy supply disruptions, exercising, and training.
- And finally, the fifth priority is to ensure that, when an incident does occur, CESER is ready to support the sector's efforts to restore the energy system efficiently and effectively.

Industrial Controls Systems Cybersecurity Initiative and Electricity Subsector 100-Day Action Plan

DOE, DHS, and the National Security Council (NSC) recently announced a Electricity Subsector 100-Day Action Plan, in partnership with the Electricity Subsector Coordinating Council (ESCC), to improve early warning and detection of cyber threats to critical energy systems across the country. This effort builds upon the successful partnerships CESER has established on threat information sharing with the electricity sector through the Cybersecurity Risk Information Sharing Program (CRISP) and research done through programs such as the Cybersecurity for the Operational Technology Environment (CyOTE) program.

Trainings and Exercises

CESER's capacity building efforts, training efforts, and exercises with energy companies and SLTT governments promote timely risk and threat information sharing, effective implementation of mitigation measures, and coordinated energy security planning. This work includes online trainings, playbooks, workshops, and guidance to help build capacity throughout the sector and ensure that SLTT energy officials and industry executives have the skills and resources they need to prepare for and respond to significant energy disruptions, including from cyber-attack.

CESER's initiatives include trainings such as CyberStrike, which helps energy sector owners and operators prepare for a cyber event by drawing on real world incidents. CyberStrike focuses on operational technology (OT) systems and networks that control operations at compressor stations and pumping sites. In November 2021, CESER will host the 7th annual DOE CyberForce Competition, which brings together hundreds of students from across the country to participate in a collegiate-level energy-focused cyber defense competition. And through CESER's Operational Technology Defender Fellowship (OT Defender), mid- to senior-level OT security managers develop a better understanding of the cyber strategies and tactics, techniques, and procedures that adversarial state and non-state actors use to target U.S. energy infrastructure.

CESER recently released an updated version of our Cybersecurity Capability Maturity Model (C2M2), a tool that helps energy companies improve their understanding of cybersecurity capabilities, gaps, and challenges. C2M2 connects business context, critical resources and

functions, and the related cybersecurity risks to enable companies to focus and prioritize their cybersecurity efforts consistent with risk management strategies and business needs.

Digital Supply Chain Security

CESER is leading the charge in addressing digital supply chain threats to industrial controls systems through our Cyber Testing for Resilient Industrial Control Systems (CyTRICS). The program identifies high priority OT used in energy systems components, performs expert testing, shares information about vulnerabilities, and informs improvements in component design and manufacturing. CyTRICS leverages facilities and analytic capabilities at four DOE National Laboratories and strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners. In 2020, CESER completed full pilot testing and focused on scaling up testing operations and adding more vendors and manufacturers. In early 2021, the program worked with DHS, in collaboration with a manufacturer, to make the first publicly announced discovery of significant cyber vulnerabilities in relays found across the energy system.

Security by Design

In May 2021, CESER kicked-off an effort to incorporate cybersecurity as a core aspect as the Department develops new technologies for the energy sector, including working closely with our partners in the Office of Electricity (OE), Office of Energy Efficiency and Renewable Energy (EERE), and the other DOE applied energy and science programs.

Further, through work on efforts such as Cyber-Informed Engineering (CIE), CESER is developing a methodology to engineer-out cyber risk from conceptual design through deployment. The methodology is being developed in partnership with Idaho National Laboratory (INL), academia, and industry. This will result in a national strategy for cyber-informed engineering that could be translated to other critical infrastructure sectors in the future.

Cyber Response

And finally, for any cyber incident affecting the energy sector, CESER coordinates across interagency, SLTT governments, and industry. CESER also assesses the potential impacts of a cyber incident and other threats on energy infrastructure. During a cyber incident, CESER leverages the world-class capabilities of the National Laboratories to provide energy systems expertise and situational awareness to interagency, SLTT, and industry partners. CESER also facilitates regulatory waivers or emergency orders to mitigate disruptions. We do this as the SRMA, under the procedures outlined in Presidential Policy Directive (PPD)-41 and the National Cyber Incident Response Plan, working to support our partners at CISA, the FBI, and the Office of the Director of National Intelligence (ODNI).

Conclusion

CESER is committed to safeguarding the Nation's critical energy infrastructure in collaboration with our public and private sector partners. Thank you for the opportunity to testify today. I look forward to your questions.