Testimony of Director Puesh Kumar

Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

Senate Energy and Natural Resources Committee

March 23, 2023

Introduction

Chairman Manchin, Ranking Member Barrasso, and distinguished members of the Committee, thank you for the opportunity to testify on behalf of the Department of Energy (DOE) on our continuing efforts to secure the nation's critical energy infrastructure. I appreciate the interest and partnership from the committee on this critical issue.

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 those threats.

The energy sector provides the power and fuel 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 safety and 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 state, local, tribal, and territorial governments (SLTT), as well as industry, with response and restoration when a disruption occurs.

Unprecedented Cyber Threats

Within the United States energy sector, an incredible transition is underway. New sources of energy generation are coming online; new digital tools and technologies are being leveraged to improve reliability and efficiency; and new market forces are shaping how we interact with energy daily, in vehicles, in homes, and in businesses across the country. With these changes come new risks and new opportunities to advance our cybersecurity posture.

The need to connect – to networks, to other devices, and to users – is driving efficiencies, cost savings, and convenience in the energy sector. New generation sources and grid capabilities necessitate new connection points and requirements to ensure the grid is reliable. Across the nation, consumers are becoming more actively involved in their energy use and are leveraging smart technology to connect. While these new connections are critically important for the U.S. energy system of the future, they are also, unfortunately, opportunities for malicious actors to disrupt those same systems for political, economic, and/or adversarial motives.

Simultaneously, cyber risks to energy systems continue to increase, from nation states, criminal actors, and other malicious cyber actors. From 2019 through 2023, each Annual Threat Assessment of the U.S. Intelligence Community from the Director of National Intelligence has pointed to persistent and malicious cyber threats facing U.S. infrastructure. These reports are clear: the cyber actors targeting U.S. energy infrastructure are a serious threat to national security.

The reports note that both Russia and China have the capability to launch cyber-attacks against U.S. energy infrastructure that could disrupt critical energy services. The 2019 Annual Threat Assessment states that, "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours..." while the 2023 Assessment says, "China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines..."

Cyber threats come in a variety of forms and, at their worst, can lead to the catastrophic failure of critical energy systems. The 2020 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 networks of critical infrastructure owners and operators, but also their suppliers and manufacturers, and exposed the level of risk one compromised piece of software can bring to bear on thousands upon thousands of networks. 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.

In 2021, Colonial Pipeline Company proactively shut down its pipeline systems for five days after a cyber-criminal group compromised the company's information technology (IT) network with ransomware. The shutdown ultimately led to a disruption in the supply of petroleum products across multiple states. The incident reminded us that, as the energy systems Americans rely on in their everyday lives grow increasingly interconnected, so too do the vulnerabilities in these systems and the potential for energy supply disruption.

In 2022, DOE, along with the Cybersecurity & Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and National Security Agency (NSA) released a joint advisory warning that malicious actors have exhibited the capability to gain full system access to multiple industrial control system (ICS) / supervisory control and data acquisition (SCADA) devices using custom-made tools. These tools could potentially enable a threat actor to manipulate the systems that American's rely upon to produce, deliver, and consume energy. This joint advisory and its implications demonstrate our adversaries' capacity to disrupt our critical infrastructure and are illustrative of the breadth and depth of the threat landscape overall.

Energy Sector Cybersecurity Roles and Responsibilities

Cybersecurity of critical energy infrastructure presents specific challenges, including the use of operational technology, spread over a wide geographic area, with minimal tolerance for downtime or service interruptions. DOE is uniquely positioned to address malicious threats facing the U.S. energy sector as the coordinating agency for Emergency Support Function (ESF) #12, under the National Response Framework, and the Sector Risk Management Agency (SRMA) for the energy sector, pursuant to Presidential Policy Directive (PPD) 21, PPD 41, and the Fixing America's Surface Transportation (FAST) Act. As the SRMA and lead for ESF #12, DOE has trusted relationships that enable us to work collaboratively with industry partners, as well as world-class subject matter experts, through the National Labs, at the forefront of operational technology cybersecurity.

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

CESER is built upon a foundation of partnerships with industry; SLTT communities; regulators like the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC); suppliers and manufacturers; and academia. I 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.

Addressing Threats to Energy Infrastructure

CESER leads several significant efforts that push the boundaries of what is possible in energy cybersecurity. We continue, with great urgency, to strengthen our sector’s cyber defenses, invest in new capabilities, and reimagine how we think about cybersecurity to ensure the resilience of the nation’s critical energy infrastructure. Given the severity of the threats we face, we must enhance cyber threat collaboration, secure energy sector supply chains, and build in security by design.

Enhancing Cyber Threat Collaboration

The congressionally chartered Cyberspace Solarium Commission and the recently released National Cybersecurity Strategy (NCS) call out the need for shared responsibility between the public and private sectors, as much of the nation’s energy infrastructure is privately owned and operated. The NCS specifically highlights DOE’s pilot of the Energy Threat Analysis Center (ETAC) as an example of the new and innovative capabilities that the nation needs to build, to effectively collaborate at the scale and speed needed to defend critical infrastructure.

In coordination with CISA and the private sector, the ETAC Pilot Program will bring experts from government and industry together to analyze and address cyber threats to the energy sector. Through this new, operational approach to cyber collaboration, we will close gaps in our collective situational awareness of threats, improve our ability to mitigate and defend against them, and support the nation’s response to incidents within the energy system.

Securing Energy Sector Supply Chains

Made possible by the leadership of this committee, the Infrastructure Investment and Jobs Act made crucial investments in the cybersecurity of our energy sector supply chains. Section 40122 of the law called upon DOE to establish an Energy Cyber Sense program to strengthen the cybersecurity of hardware and software the sector depends on to operate the energy systems of today. CESER is proud to lead this effort in partnership with the DOE National Laboratories, global manufacturers, and suppliers, energy owners and operators, and others.

We're envisioning Energy Cyber Sense to look at policies, standards, testing, educational awareness, and more to take a broad view of addressing this cyber risk. Lessons learned from this program will be shared with energy sector asset owners and manufacturers who are best positioned to address them.

A flagship initiative of Energy Cyber Sense is the Cyber Testing for Resilient Industrial Control Systems, or CyTRICS™ program, which leverages the best-in-class test facilities and analytic capabilities of the DOE National Laboratories to inform improvements that strengthen the security and resilience of hardware and software in the energy sector. CyTRICS™ partners with top manufacturers and utilities in the sector to identify systemic supply chain vulnerabilities that can help us engineer out cyber weaknesses in next-generation energy systems.

Building in Security by Design

It is far more efficient and effective to build in security measures as new technologies are designed than it is to bolt on cybersecurity solutions once hardware or software is in use. There are two major components to the effort to realize security by design in the energy sector: 1) developing cybersecurity baselines for owners and operators and 2) investing in research, development, and demonstration (RD&D) to bring new solutions to the market.

In 2022, several states began exploring the development of cybersecurity baselines for utilities operating within their jurisdiction. To prevent a patchwork approach to the implementation of cyber baselines, last month, CESER partnered with the National Association of Regulatory Utility Commissioners (NARUC) to kick-off an effort to establish a set of cybersecurity baselines for distribution electric systems and distributed energy resources. The focus is to establish cybersecurity best practices that will demonstrably buy down the cyber risk to our country's energy infrastructure. This effort will help create a more stable, more predictable business environment for energy innovators over time while having a real impact on the overall cybersecurity of our energy systems.

It is critical that our cyber research, development, and demonstration (RD&D) efforts outpace the efforts of our adversaries and that we continue to innovate faster than they can deploy. CESER is actively working to reduce risks to the electricity, oil, and natural gas systems through threat-informed RD&D of next generation tools and technologies that provide U.S. energy companies cutting-edge cyber protection, monitoring, detection, response, containment, forensics, and recovery capabilities.

In 2022, CESER released a $45 million Funding Opportunity Announcement (FOA) to strengthen the cybersecurity of next generation energy systems that will create, accelerate, and test technology to protect our energy systems from cyber attacks. Further, CESER executed a $12M FOA to establish a network of university-based, regional cybersecurity research and development centers across the nation. Finally, CESER awarded $12M for six university-based

RD&D projects focused on the development of cutting-edge cyber-physical platform tools and technologies that can detect and mitigate incidents in electric power systems.

We are also looking forward to continuing our implementation of Infrastructure Investment and Jobs Act programs this year, including the Cybersecurity for the Energy Sector Research, Development, and Demonstration Program. This $250 million program is designed to support the development and deployment of advanced cyber applications, technologies, and threat collaboration efforts through cooperative agreements and contracts with utilities, the National Labs, manufacturers, and vendors. The first FOA of this program is expected in the coming weeks.

These are areas of focus for CESER as we partner with the DOE National Laboratories, higher education institutions, manufacturers, cyber technology companies, energy companies, and others to advance cybersecurity across the United States energy sector.

Conclusion

Energy security is critical to our national security. CESER is committed to ensuring that the U.S. energy sector continues to remain secure and resilient for Americans today and for generations to come. Thank you for the opportunity to testify today. I look forward to your questions.