**Testimony of Director Puesh Kumar**

**Office of Cybersecurity, Energy Security, and Emergency Response**

**U.S. Department of Energy**

**House Energy and Commerce Committee**

**Subcommittee on Oversight and Investigations**

**May 16, 2023**

## Introduction

Chairman Griffith, Ranking Member Castor and distinguished members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Energy (DOE) on the unique role we play as the Sector Risk Management Agency (SRMA) for the United States energy sector. I appreciate the interest and support from the Committee on this critical issue.

My testimony today will focus on the value of SRMAs, the need for specialization by sector, and the role that DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) plays in fulfilling the Department's duties as an SRMA.

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 cyberattacks, physical incidents 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.

## The Evolving Threat Landscape

The U.S. energy sector faces three major types of threats: cyber threats, physical threats, and climate-related or natural threats. As the SRMA for the sector, DOE takes an all-hazards approach to risk mitigation, strategically addressing each risk individually and considering points of compounding risk, as when a natural disaster makes energy systems more vulnerable to a physical or cyber-attack.

Cyber risks to energy systems continue to increase, both from Nation states and criminal 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 threat to national security.

The reports note that both Russia and the People's Republic of 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..."

Physical threats to the energy sector come in many forms, including petty vandalism, theft, and, as we've seen more recently, targeted gun fire. Physical attacks that result in the disruption of energy flow have both economic and national security impacts and therefore this threat type cannot be underestimated or discounted.

These threats are matched, if not outpaced, by the wrath of climate-related threats such as hurricanes, wildfires, and extreme winter storms, which are happening with greater frequency and intensity year over year. DOE remains committed to working alongside our partners in the energy industry, as well as state emergency managers and community-level representatives, to plan for, prepare for, and ultimately respond to these disasters and their impacts on energy infrastructure and service. CESER and DOE more broadly are working to build resilience into the grid via new technologies, but also via strong and active partnerships that enable swift and strategic collaboration when it is needed most.

Given the immense gravity of the threats currently facing U.S. critical energy infrastructure, it is imperative that we employ a whole-of-government approach to risk management and mitigation. The SRMA model allows us to scale and to work in concert with our counterparts and with partners across the entirety of the federal government.

**The Need for SRMAs**

Protecting and securing America's critical infrastructure is a multifaceted undertaking and is best managed by those familiar with sector-specific nuances and challenges. As each SRMA is responsible for day-to-day oversight and coordination of the Federal response to risks, it is sensible to divide and conquer, putting those with the most experience and greatest expertise to meet threats head-on in leadership positions in each respective sector.

Presidential Policy Directive 21 (PPD-21), which established the SRMA structure and function within the federal government, states that "each critical infrastructure has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector."

As the SRMA for the energy sector, DOE has the "day-to-day responsibility and sector-specific expertise" to work within the sector and collaborate with the Cybersecurity and Infrastructure Security Agency (CISA) as the National Coordinator for Critical Infrastructure Security and Resilience. We value our partnership with CISA; while we bring a depth of knowledge of the energy sector and the tactical and technical elements that keep power and fuel flowing to

Americans, CISA serves an important coordinator function and has a unique perspective that is invaluable to DOE's risk management activities.

In addition, the Department of Energy has an additional responsibility to the nation as the energy sector is a critical infrastructure sector relied upon by all other sectors. In fact, PPD-21 notes "energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." Throughout PPD-21, and policies put forth by multiple administrations, the intention that SRMAs would leverage sector-specific expertise to devise and deploy solutions to some of America's greatest security challenges is clear, and the Department of Energy has consistently been recognized for our leadership in this regard.

DOE is uniquely qualified to manage the ever-changing risk landscape for America's energy sector precisely because we have a depth of knowledge specific to the generation, transmission, distribution, and consumption of energy in all its forms. We also have an exceptional breadth of capabilities across the Department, including cybersecurity and emergency response capabilities that reside within CESER, and we do not hesitate to call on the full complement of experts as needed to fulfill our duties. From nuclear physicists and security specialists to subject matter experts in renewable energy development and deployment, we regularly avail ourselves of the immense trove of knowledge readily available within DOE.

In early March, President Biden released the 2023 National Cybersecurity Strategy. In this document DOE was noted as an exemplary SRMA, pointing to the advances the Department is making in operational collaboration, the model that we set for other SRMAs, and the leadership we consistently display. DOE is not only an SRMA but is also an owner and operator of energy systems that fall under SRMA jurisdiction. With this perspective, we are able to identify issues and develop processes that efficiently and effectively address concerns across the sector.

Finally, CESER executes both Emergency Support Function #12 (ESF #12) and SRMA responsibilities on behalf of DOE 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), other agencies, and elements of the Intelligence Community.

**The Value of DOE as the SRMA**

DOE's work as the SRMA for the energy sector extends to all hazards. In recent years, several examples of the value of the SRMA have emerged from incidents or activities under DOE's purview.

In May 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. During the Colonial Pipeline incident, DOE activated it emergency response organization to coordinate with industry, interagency, and state partners, providing situational awareness, analysis of impacts, and supporting response efforts. DOE

coordinated a whole-of-government response to help Colonial resume operations quickly and safely, while moving fuel supplies to impacted areas to mitigate impacts to consumers.

In December 2022, two separate incidents involving gun fire targeting electricity substations in Moore County, North Carolina knocked out power to more than 40,000 customers. In response to these incidents, CESER worked closely with local, state, and federal law enforcement authorities, while also supporting the affected utility as they made every effort to restore power quickly. In emergent situations such as this, DOE plays a particularly critical role, serving as a hub of information flow and communication to provide utilities and other owners and operators of critical energy infrastructure visibility into potential threats and support should they be targeted.

I would be remiss if I did not mention CESER's hurricane response efforts, as we are on the brink of another hurricane season, starting on June 1. The growing intensity of hurricanes is a matter of great concern, as is their detrimental impact on American cities and communities. The provision of energy during an emergency is paramount to the rapid recovery of those affected. CESER's ESF #12 response team stands ready to deploy, to help manage restoration of power and the flow of fuel to those in need. From cyber-attacks to physical attacks, to hurricanes, and beyond, the Department of Energy is very well prepared to respond to and to manage threats to the U.S. energy sector. The work we do domestically also allows us to step up and aid our allies in times of need.

In February 2022, Putin's Russia brutally, illegally, and immorally began its full-scale invasion of the sovereign nation of Ukraine. Even before Russia attacked with tanks and troops on the ground, it had already used energy as a weapon to terrorize the Ukrainian people. Russia's use of energy as a weapon has backfired. It has spurred an international response unprecedented in the history of global energy cooperation. The United States has been a leader in this response. As part of the U.S. effort, DOE has become a reliable partner to the Ukrainian people. The Department was able to leverage our sector expertise and partnership with U.S. energy companies to support Ukrainian energy companies on both cybersecurity and grid restoration efforts during this great time of need. Further, DOE provided energy system cybersecurity training to our allies in Europe.

All this work is reliant on the health and strength of our relationships, both at the state and local levels, and with the owners and operators of America's energy infrastructure.

**An SRMA Powered by Partnerships**

In addition to working in collaboration with experts from across DOE, 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. It is through these trusted relationships that we are able to execute our responsibilities on behalf of DOE as the SRMA for the energy sector.

A large majority of the critical energy infrastructure in the United States is owned and operated by private companies. It is crucial that lines of communication between the Federal government

and these companies remain open and that we approach risk management for the sector with a sense of shared responsibility. CESER facilitates both the Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Gas Subsector Coordinating Council (ONGSCC) in partnership with DHS and other agencies, bringing representatives from the energy sector together regularly in conversation to identify security and resilience challenges and advance policy, technology, and preparedness solutions.

Similarly, CESER is extremely active on the SLTT front, providing resources and technical assistance to state-level energy and emergency managers, hosting and conducting meetings to connect the dots for state and local leaders on complex issues, and seeking opportunities for collaboration to further our collective mission of realizing a more secure, reliable, and resilient energy sector for all Americans.

Finally, CESER frequently interfaces with the DOE National Labs, organizing, funding, and leading projects to advance the security of the nation's energy systems through advanced research, development, and demonstration. The world-class subject matter experts at the Labs are part of the extensive network of resources that make the DOE the best possible SRMA for the energy sector.

It is fundamentally true that our success as an SRMA is powered by partnerships and bolstered by our unparalleled expertise and the tactical knowledge we can deploy to address incidents in real time. DOE is undoubtedly the most qualified agency to execute the role of the SRMA for the United States energy sector, both now and in the future.

**What Lies Ahead**

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.

As this transition takes place, CESER is committed to ensuring that DOE, as the SRMA for the sector, keeps pace with evolving and emerging security needs. We are actively involved with the Department's overall grid modernization activities, bringing our security expertise and experience to bear as new technology is deployed and advocating for security by design throughout the grid of tomorrow.

The value DOE brings as the SRMA in this evolving environment will be a concerted focus on innovation, collaboration, and efficiency. On behalf of the Department, CESER will continue to update our risk assessments and response operations and invest in tools and technologies to address the ever-evolving threat landscape.

According to the National Cybersecurity Strategy, the DOE pilot of the Energy Threat Analysis Center (ETAC) provides an example of the new and innovative capabilities that the nation needs to effectively collaborate at the scale and speed needed to defend critical infrastructure. 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.

DOE is adept at deploying innovative solutions to complex problems and will continue to do so in service to the American people, ensuring the U.S. energy sector becomes only more secure and resilient with time.

**Conclusion**

In closing, I would like to thank the members of this Subcommittee once more for your continued bipartisan support for SRMAs across sectors, and for DOE and CESER specifically. Your commitment to protecting America's critical infrastructure is essential for our continued success.

You understand that energy security is critical to our national security. DOE is committed to ensuring that the U.S. energy sector remains 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.