House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023, Hearing
Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies
Questions for the Record Submitted to Mr. Puesh Kumar

QUESTIONS FROM REPRESENTATIVE MORGAN GRIFFITH

Q1. Cyberattacks to critical infrastructure present one of the most significant threats to the Nation and the interconnected nature of critical infrastructure systems exposes these systems to attacks from foreign adversaries and their allies. Last year, Congress placed a "high priority on ensuring the protection of the electric grid against cyberattacks and remains concerned about the rise in frequency and sophistication of large-scale, nation state-directed attacks," in its report accompanying the House of Representatives' Energy and Water Development and Related Agencies Appropriations Bill for Fiscal Year 2023. To better enhance secure systems to strengthen defense of grids, Congress provided funding to the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) specifically "to expedite development and testing of secure inputs, processing, and outputs of systems utilizing novel cybersecurity technology." It is the Committee's understanding that this directive has not been executed. How does CESER plan to carry out this direction from Congress in an expeditious manner to better secure systems and enhance national security in the face of growing threats?

A1. The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER)'s mission is to strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions. To accomplish this mission, CESER develops tools and technologies to mitigate risks to the energy sector. CESER solicits applications to competitively select and award research and development (R&D) projects. CESER developed a Request for Information (RFI) to identify research gaps from the energy sector which includes the development and testing of secure inputs, processing, and outputs of systems utilizing novel cybersecurity technology. This RFI was released on September 5, 2023, and closed on October 11, 2023. CESER will then release a competitive solicitation, informed by the RFI, and award projects that best address the cybersecurity priorities included in the report accompanying the Energy and Water Development and Related Agencies Appropriations Bill for Fiscal Year (FY) 2023. These projects will be awarded in FY 2024.

Q2. Late last year, the Cybersecurity Infrastructure & Security Agency (CISA) released its new Cross-Sector Cybersecurity Performance Goals (CPGs), a foundational set of information technology and operational technology practices and recommendations intended to help smaller, lesser-resourced organizations better prioritize cybersecurity efforts and reduce risk. It is the Committee's understanding that CISA stated at the time

that it was going to work with Sector Risk Management Agencies (SRMAs) to develop sector-specific CPGs.

Q2a. Has CESER engaged CISA on developing these sector specific CPGs, and if so, how are those efforts progressing? When should we expect them to be done?

A2a. CESER has engaged with the Department of Homeland Security's Cybersecurity Infrastructure and Security Agency (CISA) on developing sector-specific Cyber Performance Goals (CPGs). As the Sector Risk Management Agency (SRMA) for the energy sector, CESER, on behalf of the Department of Energy, is collaborating with CISA, industry trade associations, Sector Coordinating Councils, and energy private sector partners to identify specialized concerns the energy sector has with the application of sector-specific performance goals to energy devices and processes.

This is particularly important for both Industrial Control Systems (ICS) and operational technology devices, as well as new technologies like distributed energy resources (DER). Separately from the development of the CPGs, DOE funded an effort with the National Association of Regulatory Utility Commissioners (NARUC) to develop a set of cyber baselines for Distribution Systems and DER. CISA is a partner in this effort and this work will inform the energy sector specific CPGs. CESER anticipates completing these baselines in 2023. Additionally, CESER is using concepts from that effort to inform the development of performance goals for other parts of the sector, including oil and natural gas pipelines.

Q2b. How is CESER using CISA's cross-sector CPGs to drive security improvements in the energy sector?

A2b. The energy sector is highly regulated. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards for transmission and generation entities, the TSA Security Directives for critical natural gas pipelines at the federal level, and the growing number of state public utility commission requirements provide a high bar for security controls implemented throughout the energy

sector. CESER is focusing efforts to use the CPGs as a resource for utility owner/operators who do not fall within the jurisdiction of one of the above-named frameworks. While the CPGs are performance goals, not implementable controls, CESER is focused on finding ways to use the CPGs to encourage sound cybersecurity practices and reduce risk throughout the energy sector.

Q3. How do you measure and report on the impact and outcomes of your cybersecurity initiatives and investments on cyber-physical systems in critical infrastructure?

A3. DOE has a comprehensive portfolio of activities to enhance the energy sector's cybersecurity and cyber-physical posture. The Department utilizes programmatic best practices from project identification / project selection to outcome management to secure cyber-physical systems from cybersecurity threats. Program and project progress (along with key highlights) within CESER, are tracked on a quarterly basis and reported through ongoing continuous review and improvement processes.

For example, CESER measures and reports the impact and outcomes of its supply chain cybersecurity testing efforts (CyTRICS program) quarterly under the DOE Annual Performance Goals. These metrics are available publicly on the federal government's performance management website: www.performance.gov.

In addition, CESER has measured and reported on impacts and outcomes in a 2018 report titled *From Innovation to Practice: Re-Designing Energy Delivery Systems to Survive Cyber Attacks*, which is posted on the Department of Energy's website: https://www.energy.gov/ceser/articles/ceds-rd-innovation-practice-redesigning-energy-delivery-systems-survive-cyber.

The report describes technologies that CESER developed and transitioned to the Energy Sector. Utilities nationwide have purchased risk-reducing technologies developed through this CESER-funded research.

House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023, Hearing
Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies
Questions for the Record Submitted to Mr. Puesh Kumar

Q4. What are the main challenges and gaps that hinder effective collaboration and information sharing between SRMAs and private sector stakeholders on cyber-physical threats and incidents, and what are you doing to address them?

A4. Consistent with Presidential Policy Directive 21 and the Homeland Security Act of 2002, the Secretary of Homeland Security, through the Cybersecurity and Infrastructure Security Agency, is tasked with coordinating a national effort to secure and protect against critical infrastructure risks. Sector Risk Management Agencies, such as the Department of Energy, coordinate with the Department of Homeland Security and critical infrastructure owners and operators to improve collaboration and information sharing. As the U.S. energy sector and our energy systems evolve, grow, and deploy new technologies, they face persistent cyber and physical threats from a variety of sources including nation-states, criminals, and other malicious actors — threats that the federal government and industry each have unique, critical, and complementary roles in addressing. Given that much of the Nation's energy infrastructure is privately-owned, meeting the shared responsibility to address these issues requires government and industry to work hand-in-hand.

CESER leads DOE's risk management coordination activities, including the Energy Threat Analysis Center (ETAC) Pilot which brings experts from the federal government and the energy sector together to address threats to the energy system. The ETAC Pilot addresses several long-standing challenges, including the need for intentional and ongoing integration of government and energy sector risk expertise, formalized/institutionalized collaboration on energy threat assessment at the operational level, two-way sharing of relevant and timely threat information, prioritization of energy sector risks informed by both government and private sector perspectives, and the development of collective mitigations for known risks to the energy sector.