Statement of
Alexander Gates
Senior Advisor in the Office of Policy for
Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
Before the
U.S. House of Representatives
Appropriations Subcommittee on
Energy and Water Development
March 3, 2020

Madam Chairwoman, Ranking Member, and Members of the Committee, thank you for the opportunity to appear before you to discuss the President's Fiscal Year (FY) 2021 budget for the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

CESER was created to help secure our Nation's energy infrastructure against all hazards, reduce the risks of, and impacts from, cyber events and other disruptive events, and assist with restoration activities. To that end, CESER facilitates and manages the execution of DOE's responsibilities for Emergency Support Function #12 (ESF #12) (Energy) under the National Response Framework, and is the Energy Sector-Specific Agency (SSA) for national efforts to enhance the preparedness, resiliency, and recovery of the U.S. energy infrastructure.

We are keenly aware of the cyber challenges the energy sector faces. The Director of National Intelligence stated in his 2019 Worldwide Threat Assessment that "[o]ur adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure."

"China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States. 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—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."

Due to the critical role the energy sector plays across Federal, State, and local jurisdictions, CESER programs work in an integrated manner in partnership with industry and other stakeholders, as well as other DOE offices and other federal agencies, to enhance the resilience (the ability to withstand and quickly recover from disruptions and maintain critical function) and security (the ability to reduce risks in the protection system assets and critical functions from unauthorized access and actions) of the U.S. energy infrastructure. A reliable and resilient energy

infrastructure is critical to U.S. economic competiveness, innovation, leadership, and to put it frankly, our way of life. Maturing CESER into an organization that engages with all stakeholders, especially those in the energy sector, one that focuses on functions that are inherently governmental, and takes advantage of DOE's considerable inherent strengths such as the national lab complex and its relationships within the industry, is crucial to its success.

In order to effectively align CESER's priorities with those of its stakeholders, our strategic focus concentrates on these areas:

- ***Situational Awareness*** – Obtaining, maintaining and sharing sector-wide situational awareness will benefit all levels of public and private interests in defending the energy sector. Sources of data include DOE's North American Energy Resilience Model as well as other sources from United States Government, State and Local Governments, Industry, and National Laboratories.
- ***Discovery*** – Early detection of malicious activity or dangerous devices is a critical service to the energy sector. Smart data management, advanced analytics, intelligence, and commercial products are key tools in the goal to anticipate or predict cyber attacks.
- ***Research & Development (R&D)*** – A robust, purposeful research and development approach that target gaps in the sector's capabilities is central to CESER's investment strategy.
- ***Emergency Response*** – Fulfilling the Department's responsibilities as the Coordinator for ESF #12 is a critical requirement in CESER. Increasing the Department's situational awareness and analysis capabilities will make its Infrastructure Security and Energy Restoration (ISER) division more effective and efficient.
- ***Operationalization*** – Developing processes that effectively align mission with people and technology to meet clear operational objectives is the essence of operationalizing more of the functions in CESER. Operationalizing the situational awareness mission (*what should we know, when should we know it, who should we inform*) is the highest priority.

Highlights of the FY 2021 Request

The President's FY 2021 Budget Request provides $184.6 million for CESER, a $28.6 million increase from FY 2020 enacted.

The FY 2021 budget invests in the development of tools needed to protect the U.S. energy sector against threats and hazards, mitigate the risks and minimize the extent of damage from cyberattacks and other disruptive events, and strengthen the resilience of system survivability, through the development of the capabilities to more rapidly restore power after disruptive events.

CESER works in a collaborative and integrated manner with industry, as well as Federal, state, local, tribal, and territorial (SLTT) jurisdictions, and other DOE offices, enabling industry to meaningfully enhance the security and survivability of U.S. energy infrastructure through investments across:

- R&D that delivers game-changing tools and technologies that help utilities secure today's energy infrastructure from advanced cyber threats and design next-generation future systems that are built to automatically detect, reject, and withstand cyber incidents, regardless of the threat.
- Cybersecurity tools and development that strengthen the energy sector's cybersecurity posture through public and private sector partnerships leveraging DOE-supported tools, guidelines, outreach, training, and technical assistance.
- Emergency preparedness and response that pursue enhancements to the security and resilience of energy infrastructure, and facilitate faster recovery from disruptions.

Detailed Elements of the FY 2021 Request

Cybersecurity for Energy Delivery Systems

The Cybersecurity for Energy Delivery Systems (CEDS) division seeks to reduce the risk of energy disruptions due to cyber events. CEDS' request of $103.1 million will provide valuable support for the acceleration and expansion of efforts to strengthen energy infrastructure against cyber threats and mitigate vulnerabilities. Working closely with the energy sector and our government partners, the request focuses on: 1) enhancing the speed and effectiveness of threat and vulnerability information sharing, including bi-directional machine-to-machine information sharing; 2) accelerating game-changing R&D to mitigate cyber incidents in today's systems; and 3) developing next-generation resilient energy delivery systems while developing analyses to quantify the resulting relative risk reduction.

For instance, appropriately funded research could accelerate development of artificial intelligence (AI) techniques for critical energy delivery infrastructure, such as machine learning using data generated by the underlying physical process of energy delivery and data generated by the systems that control the process, capable of providing an automatic response to cyber-attack. Such AI techniques could allow for energy delivery systems or components, such as generation plants, to automatically adapt operations and survive a cyber-attack that would otherwise disrupt energy delivery.

The increase of $8.1 million from the FY 2020 appropriation is supporting the acceleration of research and development initiatives for the Cybersecurity for the Operational Technology Environment (CyOTE™), building upon the initial successful pilot activities that tested and analyzed the scalability of the sensor-agnostic approach.

The CEDS request also includes support to the Cyber Analytics Tools and Techniques 2.0 (CATT™2.0) program. This program is designed to provide the energy sector with contextual situational awareness and actionable information, enriched with classified threat information and unique U.S. Government analytics, to support timely discovery and mitigation of advance cyber threats to the U.S. energy infrastructure. CATT™ will leverage and enhance the sector capabilities to pre-process data to filter for redundancy, anonymize/de-anonymize, and tag data from different sources into a standardized format for CATT™ analytics.

Additionally, the CEDS request includes funding for the establishment of a national physical energy system and component testing capability designed specifically to look at the vulnerabilities of the energy sector from threats such as electromagnetic pulses (EMP) and geomagnetic disturbances (GMD), a challenge that is being coordinated with the Office of Electricity.

CESER's mission of enhancing the security and survivability of the Nation's energy infrastructure cannot be achieved without both near and long-term activities that strengthen the cyber security of the energy infrastructure across the Nation.

The request is based on critical needs and a prioritization of efforts to further strengthen vulnerable energy infrastructure against cyber threats and mitigate those vulnerabilities, by focusing on enhancing the speed and effectiveness of cyber threat and vulnerability information sharing, establishing a national cyber supply chain assessment capability in partnership with industry, and accelerating game-changing R&D.

Infrastructure Security and Energy Restoration

The Infrastructure Security and Energy Restoration (ISER) division FY 2021 budget request is $70 million, an increase of $22 million from the FY 2020 enacted level. ISER is responsible for coordinating a national effort that secures U.S. energy infrastructure against all hazards, reduces impacts from disruptive events, and assists industry with restoration activities. ISER delivers critical capabilities including energy sector emergency response and recovery (including emergency response of a cyber nature); near-real-time situational awareness and contextual information sharing about the status of the energy systems to improve risk management; analysis of evolving threats and hazards to energy infrastructure; and technical assistance that incorporates exercises (e.g., tabletop exercises and simulations) in order to strengthen Federal, regional, and SLTT abilities to work more effectively together to prepare for and mitigate the disruptive impacts of an energy sector emergency. By working with the SLTT energy community to plan and develop mitigations, the Nation's energy systems will become more secure and resilient.

ISER is responsible for executing DOE's Energy SSA and ESF #12 (Energy) roles and providing DOE's support to the Infrastructure Systems Recovery Support Function. ISER also serves as the key point of entry for the energy private sector partners when collaborating with DOE and the Federal Government on critical infrastructure protection, energy security, and emergency response.

To meet its mission and support its stakeholders, ISER delivers critical capabilities including: 1) energy sector emergency response and recovery to all hazards (including emergency response of a cyber nature); 2) near-real-time situational awareness and information sharing about the status of the energy systems to improve risk management; 3) analysis of evolving threats and hazards to energy infrastructure; and 4) providing technical assistance, including exercises to strengthen Federal, regional, and SLTT capabilities, so that all may work collaboratively in preparing for and mitigating the effects of an energy sector emergency. The budget request fully supports the National Cyber Strategy and energy sector security and resilience in coordination with our

government and industry partners in the delivery of emergency response coordination, energy sector situational awareness, and cyber preparedness and incident coordination as stipulated in the 2015 Fixing America's Surface Transportation (FAST) Act, as well as by providing critical seeding for public-private partnerships at the National Laboratories, advancing the Department and its partners' efforts to prepare for, mitigate, respond to, and recover from all threats and hazards facing the U.S. energy sector.

ISER will continue to maintain and improve its ability to support industry and interagency coordination during major disruptive events, such as hurricanes, wildfires, and cyber-attacks, and will develop subject-specific training for responders that may be used and drawn upon when responding to events. We will focus on expanding familiarity with, and capability to, support remote location responses, educating responders to changing energy sector interdependencies, and expanding access to available subject matter expertise across DOE.

ISER will expand the current configuration of its situational awareness visualization platform, EAGLE-I™, and work to ensure its continued usefulness as a collaborative platform for historic and real-time data collection, integration, and curation across the public and private sectors. EAGLE-I™ will leverage cloud computing infrastructure to further scale implementation for facilitated access to existing models and data sets, thereby expanding its capabilities and value to response partners. EAGLE-I™ will also incorporate machine learning for all-hazards event characterization and consequence analysis, including cyber events. It will take advantage of high-performance computing and artificial intelligence technologies to analyze large data sets (such as historical outages and infrastructure interdependencies), improving energy sector impact prediction capabilities.

Additionally ISER will continue working with Department of Homeland Security (DHS) to proactively connect energy companies to DHS response teams before a disaster to plan and support the staging of restoration activities, enabling more rapid response to cyber incidents, working toward the goal of obtaining pre-approved requests for technical assistance from the most critical U.S. utilities.

ISER will also expand its CyberForce Competition to support the development of collegiate-level skills and persistent interest in critical infrastructure cybersecurity nationwide in support of the Administration's Executive Order 13870 America's Cybersecurity Workforce. To continue support the industry's existing workforce, ISER will greatly expand its CyberStrike training which is focused on understanding and managing the multifaceted interdependencies between the Nation's energy infrastructure and other critical infrastructure, detecting and responding within compressed timelines to prevent highly impactful consequences, and develop top-tier defenders to mitigate sophisticated threat actors.

Finally, the Cybersecurity Testing for Resilient Industrial Control Systems (CyTRICS™) program serves as a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical components to identify and mitigate embedded cyber vulnerabilities across the energy sector. Analysis of test results will identify systemic and supply chain risks and vulnerabilities to the sector by correlating collected test data

and enriching it with other pertinent data sources and methods. DOE will collaborate with other Federal partners, the National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, collaborative approach to these efforts.

Conclusion

The establishment of CESER is the result of the Administration's commitment to, and prioritization of, energy security and national security. Our long-term approach strengthens our national security and positively impacts our economy. Since establishing CESER, DOE has been working on numerous fronts collaborating with the National Laboratories, industry, and state and local governments with the unwavering commitment of identifying and mitigating the vulnerabilities of our electric grid and protecting our Nation's critical energy infrastructure from the most serious threats.

As CESER moves forward, we continue the change necessary to achieve the Administration's priority of emergency preparedness and rapid, coordinated response to disruptions in the energy sector from all hazards, including this growing cyber threat, and advancing R&D in this space to enhance the security of energy delivery systems.

I appreciate the opportunity to appear before this Committee to discuss cybersecurity in the energy sector. I look forward to working with you and your respective staffs to continue to address cyber and physical security challenges.