Testimony of Alexander Gates

Senior Advisor in the Office of Policy for
Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy

Before the

Committee on Energy and Natural Resources
United States Senate

August 5, 2020

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for the opportunity to appear before you to discuss the Department of Energy's (DOE) important work to protect the critical infrastructure of the energy sector from cyber threats. A majority of the efforts in this regard are led by the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) with support from the Office of Electricity (OE).

The DOE and its numerous partners in the Federal, State, local governments, private sector and national laboratory community are keenly aware of the numerous and complex cyber challenges that the energy sector faces. One of the most noteworthy challenges is that our adversaries are conducting an increasing number of malicious cyber activities against our nation's infrastructure, which poses a persistent threat to our nation's security and economy. These ongoing campaigns demonstrate the continued need to use the full range of legal authorities and technological capabilities afforded to the U.S. Government, including strengthening our national resilience through cyber defense and close cooperation with the private sector.

Given the Nation's growing dependence on the energy sector to power every aspect of our lives, and the increasing interdependencies of the sector on communication systems and other critical infrastructures, a major attack could cause wide-ranging national security and economic impacts. Our Nation's electricity and fuel delivery systems are complex and interdependent. There is a great potential for negative and cascading impacts when operator error, software upgrades, and equipment failures occur in formerly isolated environments. As a result, energy cybersecurity and resilience are among the Nation's most urgent security challenges.

A reliable and resilient energy infrastructure is critical to U.S. economic competiveness, national security, and the American way of life. The DOE is continually seeking to increase this reliability and resiliency by ensuring engagement with all stakeholders, particularly those in the energy sector. We also seek to take advantage of DOE's considerable strengths such as the national lab complex and our relationships across industry and State and local governments.

Within the DOE, CESER and OE work together to provide products and services to improve the energy sector's cybersecurity and resilience. The close collaboration between the two offices

improves the seamless nature and impact of the solutions that the Department offers to the energy sector.

Office of Cybersecurity, Energy Security, and Emergency Response

The mission of CESER is to improve the security of the United States energy infrastructure against all hazards via two main divisions of the Office: Cybersecurity for Energy and Delivery Systems, and Infrastructure Security and Energy Restoration. CESER's mission to improve the security and survivability of the Nation's energy infrastructure cannot be achieved without both near- and long-term activities that strengthen the cybersecurity of the energy infrastructure across the Nation. In order to achieve these outcomes, the DOE has developed and prioritized CESER's goals as follows:

- **Build a Superior Workforce** – CESER will recruit, hire, retain, train, and organize resources with a focus on deepening and sustaining technical knowledge in Industrial Control System Cybersecurity across the Department, and will help enable industry to do the same.
- **Modernize Emergency Response & Recovery** – CESER will continue efforts in modernizing DOE's capabilities to respond to all hazards in close coordination with Federal interagency partners, infrastructure owners and operators, and State and local governments by expanding skills and using new and different technologies and products – informed by lessons learned from current and recent incidents.
- **Develop Cyber Discovery** – CESER will enhance sector-wide situational awareness and cultivate multi-faceted threat intelligence to support timely and appropriate action. CESER will convene stakeholders to jointly establish operational cybersecurity processes and apply technology and products to enhance predictive capabilities to prevent cyber incidents in the energy sector.
- **Improve Situational Awareness** – CESER will continuously improve energy sector situational awareness capabilities through development of consensus driven stakeholder requirements, application of predictive analytics, integration and optimization of technology platforms, and closely linking R&D investments and sector needs.
- **Focus Research & Development** – CESER seeks to accelerate the impact of the world-leading capabilities resident in the DOE Labs and partners by: constantly evaluating the current portfolio, ensuring that R&D advances other strategic goals, addressing emerging vulnerabilities, and sizing resources and organizational structure appropriately.
- **Strengthen Partnerships** – CESER will heighten its collective impact through streamlining communication and outreach, providing products and expertise to support timely risk and threat information sharing, and training to build sector capacity.

<u>Office of Electricity</u>

OE works to provide a secure and resilient power grid which is vital to our national security, economic security, and the services Americans rely upon. Working closely with private and public partners, OE acts to ensure the nation's most critical energy infrastructure is resilient and

able to recover rapidly from disruptions. Under the leadership of the Assistant Secretary for Electricity, the organization is focused on long-term research and development to build a secure and resilient power grid. OE has four strategic priorities:

- **Build Advanced Modeling Capability -** Working with the national labs and relevant stakeholders, OE is developing an integrated North American Energy Resiliency Model (NAERM) to conduct planning and contingency analysis to address vulnerabilities in the North American energy system.

- **Advance Megawatt Scale Grid Storage -** OE is pursuing megawatt scale storage capable of supporting frequency regulation, ramping, and energy management for bulk and distribution power systems.

- **Improve Grid Operations and Performance through advanced Sensing Technology -** OE is pursuing integration of high-fidelity, low-cost sensing technology for predictive and correlation modeling for electricity.
- **Secure Defense Critical Electric Infrastructure -** OE is implementing the authorities provided under the Fixing America's Surface Transportation Act (FAST Act) to define and secure Defense Critical Electric Infrastructure (DCEI). DCEI is defined as any electric infrastructure located in any of the 48 contiguous States or the District of Columbia that serves a facility designated by the Secretary of Energy to be: 1) critical to the defense of the United States, and 2) vulnerable to a disruption of the supply of electric energy provided to such a facility by an external provider, but is not owned or operated by the owner or operator of such facility.[1] Similarly, these two conditions also constitute the definition of critical defense facilities.

Key DOE Initiatives

Further Understanding and Testing the Resilience of Our Industrial Controls

CESER's Cybersecurity Testing for Resilient Industrial Control Systems (CyTRICS™) program serves as a central capability for the DOE's efforts to increase energy sector cybersecurity and reliability through the 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. The DOE has signed multiple agreements with energy sector partners to grow the CyTRICS™ program from a proof of concept to a robust supply chain cybersecurity program for the sector. We will continue collaborating with other Federal partners, the DOE Labs, and industry to identify key energy sector industrial control systems components and apply a targeted, collaborative approach to these efforts.

[1] *See* 16 U.S.C 824o-1(a)(4).

Bulk Power Executive Order

The bulk-power system (BPS) is the backbone of the U.S. electric grid, which is critical to our national security, the economy, and way of life. As outlined in the *Office of the Director of National Intelligence 2019 Worldwide Threat Assessment* and the *2020-2022 National Counterintelligence Strategy*, foreign adversaries continue to develop new ways to compromise the BPS and the supply chain of critical components, thereby undermining national security.

To confront this increasingly sophisticated threat, the President signed Executive Order (EO) 13920 "Securing the United States Bulk-Power System" on May 1, 2020, authorizing the Secretary of Energy, working with other Federal departments and agencies, and private industry, to quickly and proactively protect the BPS.

The DOE is in the process of operationalizing EO 13920 through four "pillars" of implementation:

1) prohibiting particular foreign adversaries from supplying particular BPS electric equipment;
2) establishing a list of pre-qualified vendors of BPS electric equipment;
3) developing advisory recommendations for the identification, isolation, monitoring, and replacement of at-risk equipment currently on the system; and
4) presiding over the Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security.

Immediately after the May 1st signing of the EO, OE and CESER began an extensive outreach campaign, which ultimately resulted in 50 briefings with more than 2,300 participants from more than 900 organizations. With the intent of being as inclusive as possible, briefing participants included representatives from industry, associations, and the Federal family.

Many practitioners within the cybersecurity field often have accurately asserted that you cannot protect what you do not know you have. This was one of the rationales behind EO 13920. Accordingly, through the efforts of the DOE and its stakeholders in implementing the EO, we will unlock a new degree of critical visibility into how best to prioritize our collective efforts to address the threats.

North American Energy Resilience Model

The DOE, in accordance with its responsibility and authority to identify, minimize, and respond to risks facing the United States energy sector, has begun development of the NAERM. The NAERM is best defined as a set of modeling capabilities for the analysis of risks and threats to the grid, and other interdependent infrastructures. Unlike the status quo, the NAERM will equip the DOE with the capabilities needed to quickly assess the resilience of the electrical grid and inform the Secretary with the real-time holistic situational awareness required to address emergencies as they unfold.

Developed in coordination with eight DOE Labs, the NAERM is the first of its kind, and the foundation for analyzing the North American electric power system and its interdependencies with other infrastructures in real-time, such as natural gas and communications. When complete, NAERM will address both long-term energy planning and energy planning and operational studies with real-time data streams, national-level situational awareness for both infrastructure and threats, and analytic and decision support capabilities to anticipate threats and mitigate their impacts.

Developing and Identifying the Energy Cybersecurity Workforce of Today and Tomorrow

Cybersecurity workforce development is a national priority outlined in the President's National Cyber Strategy and Executive Order on America's Cybersecurity Workforce (Executive Order 13870). Through its CyberForce Competition, the DOE seeks to identify and develop the next generation of cybersecurity professionals who will secure the nation's critical energy infrastructure. In November 2019, the DOE held its fifth CyberForce Competition hosted by 10 National Laboratories and featured a professional-level pilot which included scoring that will be considered to identify highly qualified individuals for potential employment with the DOE. In 2019, 105 collegiate teams from 32 states and Puerto Rico participated in the CyberForce Competition, a nearly 67% increase in participation over the prior year's 63 teams from 24 states and Puerto Rico. CyberForce 2020 will be held virtually on November 14th and will focus on assessing the skillsets of individual competitors representing their respective academic institutions.

Key Partnerships

The Departments of Defense and Homeland Security and the Intelligence Community are crucial partners in the effort to protect the nation's energy infrastructure from cyber threats. The DOE holds regular discussions with energy sector Information Sharing and Analysis Centers (ISACs) to share emerging and potential threats and disseminate information. A critical DOE role is our work with State officials to facilitate state-industry preparedness and response coordination, encourage response plans that help prepare for any potential consequences of a cyber-attack, and to offer training and exercises to ensure that the States are ready and able to mitigate incidents and respond, if needed.

The DOE also works closely with our public and private partners to support and bolster the actions that are needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the Sector Coordinating Councils to synchronize government and industry cyber incident response playbooks.

Conclusion

The President recognized the threat to the energy sector, and through EO 13920 "Securing the United States Bulk-Power System", is empowering the DOE to take bold action. The Secretary of Energy has proven his continued commitment to reliable and resilient energy infrastructure, and through CESER is bolstering the DOE's collaboration with industry and State and local governments to protect our Nation's critical energy infrastructure from all hazards, including the growing cyber threat. Our long-term approach will strengthen our national and energy security and protect the American way of life.

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 physical and cybersecurity challenges to the energy sector, and welcome any questions you may have. Thank you.