Testimony of Assistant Secretary Karen S. Evans

Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

Before the Committee on Science, Space, and Technology

Subcommittee on Energy

United States House of Representatives

July 17, 2019

Introduction

Chairman Lamb, Ranking Member Weber, and Members of the Subcommittee, it is an honor and a privilege to serve at the Department of Energy (DOE or the Department) as Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). Thank you for the opportunity to testify on behalf of the Department.

A reliable and resilient electric grid is critical to U.S. economic competiveness and leadership, as well as the overall safety and security of our Nation. However, our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state- and non-state-sponsored. The frequency, scale, and sophistication of cyber threats continue to increase. Cyber incidents have the potential to disrupt energy services, damage highly specialized equipment, and even threaten human health and safety.

Earlier this year, the Office of the Director of National Intelligence released the Worldwide Threat Assessment, which noted Russia "is now staging cyber attack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis…" and "…has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effect on critical infrastructure – such as disrupting an electrical distribution network for at least a few hours…" Similarly, it noted that "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." [1]

One of the most critical missions at DOE is developing the science and technology to successfully counter the ever-evolving, increasing threat of cyber and other attacks on our networks, data, facilities, and infrastructure. DOE works closely with our Federal agency, State, local, tribal and territorial (SLTT) governments, industry, and National Laboratory partners to accomplish this mission.

[1] Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community (January 29, 2019): p.5-6

Below are some highlights and perspectives regarding the legislation being discussed today, followed by highlights of the work we are doing to advance the modernization and protection of our electric grid.

Grid Modernization Research and Development Act of 2019

The Grid Modernization Research and Development Act of 2019 focuses on eight areas, including enhancing grid resilience and emergency response; smart grid modeling, visualization, architecture, and controls; a technology demonstration grant program; grid-scale energy storage; hybrid energy systems; grid integration; grid cybersecurity (H.R. 4120 from 115th Congress); and protection of sensitive grid information.

Maintaining a modern, flexible, and secure network of electric power transmission and distribution lines, oil and natural gas pipelines, and storage facilities is essential to keeping energy accessible and affordable for businesses and consumers, promoting growth across all sectors, and supporting the continued health of the country's domestic energy industry.

Since taking office, the President has prioritized ensuring our infrastructure keeps pace with our energy abundance. He announced the Civil Nuclear Review to enable revitalization of the nuclear energy sector, while supporting R&D efforts on behalf of renewables, storage, and energy efficiency.

The Department has provided technical comments on this bill.

H.R. 4120 - Grid Cybersecurity Research and Development Act

This bill directs the Secretary to coordinate with appropriate Federal agencies, the Electricity Subsector Coordinating Council (ESCC), SLTT governments, private sector vendors, and other relevant stakeholders to:

- Carry out a research, development, and demonstration initiative to harden the electric grid and mitigate the consequences of cyber attacks by increasing the cybersecurity capabilities of the electricity sector and accelerating the development of cybersecurity technologies and tools.
- Coordinate the development of guidance documents for research and demonstration activities to improve the cybersecurity capabilities of the electricity sector through participating agencies.
- Leverage the research facilities and expertise of the National Laboratories to utilize voluntary vulnerability testing and provide technical assistance to increase cyber resilience.
- Develop education and workforce training research and standards by identifying core skills used by electricity sector industrial control systems cybersecurity professionals; and develop assessment methods and tools to identify existing personnel that show competence in those skills.
- Work in collaboration with the Secretary of Homeland Security, other appropriate Federal agencies, and energy sector stakeholders to conduct a study to analyze cyber

attacks on electricity sector industrial control systems and identify cost-effective opportunities to improve cybersecurity.

The Department is reviewing the proposed language, and we look forward to working with the Committee. DOE applauds Congress for recognizing that our national security depends on a resilient electric grid, and that reducing the risks to this critical infrastructure is one of our Nation's most urgent security challenges.

Another critical mission for DOE is ensuring the resilience of our electric grid and successfully countering the ever-evolving and increasing threat of physical and cyber-attacks on networks, data, facilities, and infrastructure.

CESER was established to help research and develop the tools and best practices to make our electric power grid and other energy infrastructure more resilient to these threats.

DOE recently announced an $8 million investment in innovations that will enhance the reliability and resiliency of our nation's energy infrastructure. This R&D partnership opportunity will spur the development of the next generation of tools and technology that will become widely adopted throughout the energy sector.

As we protect our infrastructure from cyber threats, we are also working to improve the complete resilience of our electricity systems.

Our Office of Electricity also supports transmission system resilience and generation diversity, and is exploring new architecture approaches for the electric grid. This includes the development of the North American Energy Resilience Model that aims to provide unique and ground-breaking national-scale energy planning and real-time situational awareness capabilities to enhance security and resilience.

A large component of DOE's work is pursuing cutting-edge innovation in big data, A.I., and grid-scale energy storage based on new technology.

Grid-scale storage will be an important enabler for renewable integration and for clean baseload power. While today's technologies are already providing value to the grid, there are physical limitations to traditional batteries and pumped hydro that will be surpassed by next-generation technologies.

Efforts in grid-scale energy storage are already producing important advancements. Grid-scale energy storage technologies have been demonstrated using a new generation of advanced flow batteries, which rely on lower cost electrolytes.

We are also continuing to advance energy storage through our Advanced Energy Storage Initiative (AESI), which includes development of a new Grid Storage Launchpad aimed at accelerating materials development, testing, and independent evaluation of battery technologies for grid applications.

In addition, the R&D at DOE's National Laboratories supports the development of technologies that strengthen and improve energy infrastructure so that consumers have access to reliable and secure sources of energy.

Another program driving enabling technologies is DOE's Grid Modernization Initiative (GMI), which focuses on integrating an increasing amount of variable generation into the grid through R&D infrastructure investments at our National Labs. One noteworthy GMI effort will accelerate the conversion of the National Wind Technology Center campus into an experimental micro-grid capable of testing grid integration at the megawatt scale.

These are just some of the examples of how the United States is approaching its commitment to updating and improving its energy infrastructure and environmental responsibility within its own border, but these same issues are also at the heart of so many of our partnerships and work abroad.

Energy Storage

Energy storage is a technology of national interest and the backbone of a future resilient energy system. With benefits extending to transportation, the power grid, and throughout the economy, DOE has been proactive in developing new tools and technologies to accelerate energy storage development, such as through GMI, AESI, and the Grid Storage Launchpad (GSL).

In May of this year, DOE issued its most recent Grid Modernization Lab Call, with Energy Storage and System Flexibility as one of the major topic areas. The lab call placed a particular emphasis on developing the storage functions that enhance system resilience and flexibility.

The proposed GSL will extend U.S. R&D leadership in energy storage through validation, collaboration, and acceleration. By validating new technologies at earlier maturity stages, the GSL will lower the time and expense of storage chemistry innovations. Through collaboration with universities and the commercial sector, the GSL will augment the industry with enhanced testing protocols and in-operando characterization capabilities. Finally the GSL will accelerate and de-risk new technologies by propagating rigorous grid performance requirements to all stages of storage development, from benchtop to systems.

DOE established the Mission Need for the GSL at Critical Decision 0 (CD-0) in November of 2018. We anticipate finalizing the preferred alternative facility and cost range as part of CD-1 this summer.

The FY 2020 Budget requested funds for design and construction planning of the GSL. The FY 2020 Budget also proposes an AESI led by DOE's Offices of Electricity (OE) and Energy Efficiency and Renewable Energy (EERE), in conjunction with the Offices of Fossil Energy (FE) and Nuclear Energy (NE). AESI will provide a platform to coordinate R&D activities across these programs—and existing energy storage efforts in the Office of Science (SC) and the Advanced Research Projects Agency (ARPA-E)—to establish aggressive, achievable, and measurable goals for cost-competitive energy storage technologies, services, and applications. In

FY 2020, AESI will establish application-specific cost and performance metrics to align research objectives and to coordinate the development of new energy storage and flexibility technologies.

Finally, OE's Energy Storage Program continues to conduct research and development to expand storage capabilities and shared industry knowledge. From performance breakthroughs in batteries based on earth-abundant materials to evaluation tools and workshops for state regulators, OE is at the forefront in helping communities realize the benefits of energy storage.

CESER

CESER leads the Department's efforts to 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. This office works closely with the private sector, as well as Federal and SLTT government partners, to enable more coordinated preparedness and response to cyber and physical threats and natural disasters. The office enhances the Department's ability to dedicate and focus attention on DOE's Sector-Specific Agency (SSA) responsibilities. DOE is the lead SSA for cybersecurity for the energy sector as provided in the Fixing America's Surface Transportation Act of 2015 (P.L. 114-94). CESER provides greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework overseen by the Department of Homeland Security (DHS).

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

The release of the President's National Cyber Strategy (NCS) in September 2018 demonstrates the Administration's commitment to strengthening our Nation's cybersecurity capabilities, specifically securing critical infrastructure. The NCS prioritizes risk-reduction activities across seven key areas, including national security and energy & power. DOE's cybersecurity activities for the energy sector align to the Secure Critical Infrastructure section of Pillar I – (Protecting the American People, the Homeland, and the American Way of Life) under the category to Prioritize Actions According to Identified National Risks. It states: "The Federal Government will work with the private sector to manage risks to critical infrastructure at the greatest risk. The Administration will develop a comprehensive understanding of national risk by identifying national critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks."

The strategy presents a risk-reduction-based approach to improving the Nation's cybersecurity posture in key areas, and builds on DOE's ongoing collaboration with other agencies and private sector organizations, including the Federal Government's designated lead agencies for coordinating the response to significant cyber incidents: DHS, acting through the National Cybersecurity and Communications Integration Center (NCCIC), and the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI) and its National Cyber Investigative Joint Task Force. In the event of a significant cyber incident in the energy sector, DHS and DOJ coordinate with DOE to ensure its deep expertise with the sector is appropriately leveraged.

DOE is also working with the Tri-Sector Executive Working Group (TEWG) in conjunction with the Department of the Treasury and DHS, along with our industry partners, to address and manage risks across the energy, telecommunications, and financial sectors. The formation of the TEWG was recommended by the President's National Infrastructure Advisory Council (NIAC) in their August 2017 report titled, "Securing Cyber Assets: Addressing Urgent Cyber to Critical Infrastructure."

In the energy sector, the core of critical infrastructure partners is represented by the ESCC, the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and DHS, is where the interagency partners, States, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures that we are working together in a whole-of-government response.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council framework, which provides a mechanism for industry and government coordination. The public-private critical infrastructure community engages in open dialogue to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

DOE's Cybersecurity Activities for the Energy Sector

DOE plays an active role in supporting energy sector cybersecurity by enhancing the security and resilience of the Nation's critical energy infrastructure. To address these challenges, it is critical for us to be proactive and cultivate a secure energy network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to identify, detect, protect, respond, and recover. The Department is focusing cyber support efforts to strengthen energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate game-changing research, development, and deployment (RD&D) of resilient energy delivery systems.

Strengthening Energy Cybersecurity Preparedness

It is necessary for partners in the energy sector and the government to share meaningful and timely emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber attacks more rapidly. CESER is working with government partners and the energy sector to develop a secure platform to provide energy sector-wide situational awareness and actionable information to support the discovery and mitigation of advanced cyber threats to U.S. critical energy infrastructure. The Cyber Analytics Tools and Techniques (CATT^{TM} 2.0) program will achieve this through automated analysis of voluntarily provided energy sector information technology (IT) and operational technology (OT) data, enriched with classified threat information utilizing unique and sophisticated U.S. Government tools.

Advancing the ability to improve situational awareness of OT including Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems is the key focus of DOE's current activities. Detecting adversary tactics, techniques, and procedures within anomalous traffic on critical energy infrastructure can be the first step in stopping an attack in its early stages. The Department is working with our private sector partners to develop the capability to analyze the data from OT systems via the Cybersecurity for the Operational Technology Environment (CyOTE^{TM}) pilot project. The CyOTE^{TM} pilot will develop into a scalable program for industry to aid in detecting and mitigating cyber risks to OT systems.

Additionally, CESER is implementing a threat-informed, engineering-centric assessment and mitigation activity for the energy sector called Consequence-driven Cyber-informed Engineering (CCE), which is being supported by the Idaho National Laboratory (INL). The methodology prioritizes high-consequence risks within control systems environments, identifying the most severe consequences, and then identifies the best process design and protection approaches for eliminating the cyber risk. The lessons collected from the upcoming engagements within the energy sector will be shared with our partners to greatly expand the Nation's ability to "engineer out" the cyber risk from the most critical energy infrastructure networks and systems.

Cybersecurity vulnerabilities of key control systems and operational technology are an increasing concern for the Nation's critical energy infrastructure owners and operators. The Cyber Testing for Resilience of the Industrial Control Systems (CyTRICS) program will serve as a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical electrical components. Further, analysis of test results will identify both systemic and supply chain risks and vulnerabilities to the sector through the linkage of threat information with supply chain information and enriching it with other data sources and methods. Through CyTRICS, DOE continues to collaborate with government, the National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, prioritized, and collaborative approach to these efforts.

CESER's efforts to develop a collective understanding of systemic and supply chain risks and vulnerabilities are aligned with Executive Order 13873 "Securing the Information and Communications Technology and Services Supply Chain," and support the Administration's priority of securing our Nation from foreign adversaries who are increasingly creating and exploiting U.S. vulnerabilities in information and communications technology.

Facilitating Cyber Incident Response and Recovery

As the Energy SSA, DOE works at many levels of the electricity industry. We interact with numerous stakeholders and industry partners to share both classified and unclassified information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security and reliability. By partnering through working groups between government and industry at the national, regional, State, and local levels, DOE facilitates enhanced cybersecurity preparedness.

As a member of the National Security Council and as the Energy SSA, DOE assesses and analyzes credible threats to reliability and resilience issues facing the security of our Nation's electrical grid. These intelligence assessments and analysis often involve classified information;

however, DOE works to provide regular unclassified threat briefings to interagency and industry partners, in addition to classified threat briefings to cleared members of the sector.

DOE also maintains a close relationship with the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) to ensure they have the relevant information to execute their missions. DOE also holds regular discussions with three energy sector Information Sharing and Analysis Centers (ISACs) – which include the Electricity ISAC (E-ISAC) – to share emerging and potential threats and disseminate information.

CESER also recently supported the National Governors Association (NGA) in providing Governors and their energy advisors with policy strategies to protect electricity infrastructure and enhance cybersecurity in the electricity sector. The NGA white paper outlines the roles and responsibilities of key State, industry, and Federal entities and catalogs useful resources.[2]

DOE continues to 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 offer training and exercises to ensure the states are ready and able to mitigate incidents and respond, if needed.

DOE also works closely with our public and private partners with the goal of fully supporting and bolstering the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the Sector Coordinating Councils (SCCs) to synchronize government and industry cyber incident response playbooks.

CESER engages directly with our government and industry partners to help ensure we are prepared and coordinated in the event of a cyber incident to the industry. The success of the 2018 iteration of DOE's Liberty Eclipse cybersecurity exercise developed in two phases. Phase I was a tabletop exercise focusing on the roles, responsibilities, and authorities of Federal, State, and energy industry partners in response to a significant cyber attack on energy infrastructure.

Phase II included a seven-day, operations-based exercise conducted on Plum Island in New York. This exercise focused on increasing the country's ability to mitigate adversary cyber degradation of the grid's restoration capability. During Phase II, DOE worked with the Defense Advanced Research Projects Agency (DARPA) and multiple U.S. utilities to test and evaluate tools and capabilities that could enable the recovery of the power grid during a cyber attack. These experiments were held in an isolated and controlled environment with first responders and power engineers on hand. DOE's private sector collaboration ensures DARPA's research results are directly transitioned to industry and translated into greater preparedness to a cyber attack.

[2] NGA White Paper, Smart and Safe, State Strategies for Enhancing Cybersecurity in the Electric Sector (June 2019). https://www.nga.org/wp-content/uploads/2019/04/NGA-Smart-Safe-State-Strategies-for-Enhancing-Cybersecurity-in-the-Electric-Sector.pdf.

DOE continues to sponsor Clear Path, an annual all hazards focused exercise series. These regionally-focused exercises highlight the interdependencies between our Nation's energy infrastructure and other sectors.

DOE's most recent exercise, Clear Path VII, took place in Memphis, Tennessee, in April 2019. This iteration examined the energy sector's response and restoration roles, responsibilities, plans, and procedures following a major earthquake along the New Madrid Seismic Zone. The exercise brought together more than 160 individuals from more than 80 organizations representing Federal and State governments, the electricity and oil and natural gas subsectors, and the transportation, water, and communications sectors.

It is critical that the results of the exercises inform our response plans on a continuous basis to close identified gaps in coordination with our industry and government partners through the associated coordinating councils. Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinating various efforts showcased in the exercise, including unity of messaging required to recover from a real-life version of the exercise scenario.

In preparation for any future grid security emergency, it is critical we continue working with our government and industry partners to further shape the types of orders that may be executed under current authorities, while also clarifying how we communicate and coordinate the operational implementation of these orders. Continued coordination with Federal, SLTT, and industry partners and participation in preparedness activities like Clear Path enable DOE to identify gaps and develop capabilities to support cyber response.

Accelerating Breakthrough RD&D of Resilient Energy Delivery Systems

A key to CESER's efforts to secure the Nation's electric grid against cyber attacks is supporting DOE's Grid Modernization Initiative. The Grid Modernization Initiative is introducing new technologies to better manage increasingly complex transmission and distribution systems. CESER has a central role in the Department's plan for integration of cybersecurity activities across DOE, and coordinates with other DOE offices through the Grid Modernization Laboratory Consortium (GMLC). An Executive Committee comprised of DOE leadership oversees the GMLC, through which we engage our leading experts and resources at DOE National Laboratories, collaborating on the goal of modernizing the Nation's electric grid. GMLC employs an integrated approach to ensure that DOE-funded studies and research and development are coordinated efficiently to reap the greatest return for the taxpayer dollar.

Through the GMLC, DOE's National Laboratories are assembling technical expertise to address specific cybersecurity challenges facing the electric grid. For example, GMLC is developing advanced analytics of cyber data to assist in differentiating between cyber and non-cyber-caused incidents.

In alignment with 2019 Executive Order 13865, "Coordinating National Resilience to Electromagnetic Pulses" (Mar. 26, 2019), CESER also works closely with the private sector, as well as Federal and SLTT government partners to enable more coordinated preparedness for and response to disruptions caused by electromagnetic pulses (EMPs) and geomagnetic disturbances (GMDs). An EMP can be created by non-nuclear events and by the high-altitude detonation of a nuclear weapon, which have the potential to damage power delivery assets and impact bulk-power system reliability over a wide area. GMDs, caused by Coronal Mass Ejection from the Sun, may result in geomagnetically-induced currents (GIC) in man-made structures such as rail lines, pipelines, electric transmission lines, and some communications lines. DOE is concerned about the impacts of GIC flows on power transformers. Transformer damage, although highly unlikely even in the most extreme storms, is possible and in certain situations can destabilize the electric grid if proactive measures are not undertaken (*e.g.*, reducing load).

CESER is leading efforts within DOE to address EMP and GMD risks, using a multi-pronged approach: sharing knowledge and expertise with industry on a timely basis; allowing the electric subsector to advance readiness for potential EMP impacts through research to quantify the risk; and scientific development of mitigation strategies, and analysis of the policies needed for the future. CESER is fully committed to helping forge the grid of the future that will be more resilient to all hazards, including EMP/GMD. Continued progress in grid modernization is vital to helping us protect the grid from EMP/GMD.

Cybersecurity for energy control and OT systems is vastly different from typical IT systems. OT power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time-consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly-accessible areas, where they can be subject to physical tampering. Real-time operations are imperative, and latency is unacceptable for many applications. Immediate emergency response capability is mandatory, and active scanning of the network can often be difficult.

To select cybersecurity R&D projects, DOE constantly examines the threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects.

CESER's Cybersecurity for Energy Delivery Systems (CEDS) R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused, early-stage research and development effort. CESER co-funds industry-led, National Laboratory-led, and university-led projects with SLTT and industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber incident for our present and future energy delivery systems. In a demonstration of our coordination with other Federal agencies, two of the university-led collaborations are funded in partnership with DHS Science and Technology.

In April 2019, CESER released the "Cybersecurity for Energy Delivery Systems (CEDS) 2019 Research Call" to conduct research, development, integration and demonstrations (RDI&D). This RDI&D will lead to (1) next generation tools and technologies, (2) techniques to implement cybersecurity frameworks and (3) integration of tools and technologies to help provide greater situational awareness that is unavailable today. It will likely become available and widely adopted throughout the energy sector to reduce the risk that a cyber incident could disrupt energy delivery. An estimated $35 million in Federal funding is expected to be available for new awards under this research call.

In May 2019, CESER issued an $8 million funding opportunity announcement seeking innovative approaches to enhance the reliability and resilience of the Nation's energy infrastructure. This includes enhancing the ability of electricity generation, transmission and distribution infrastructure, as well oil and natural gas production, refining, storage, and distribution infrastructure to survive a cyber attack while sustaining critical energy delivery functions. This funding opportunity supports the Administration's directive to secure critical infrastructure as outlined in the National Cyber Strategy, through research and development of real-time intrusion detection, self-healing energy delivery control systems, and innovative technologies that enhance cybersecurity in the energy sector.

Existing CESER projects in Artificial Intelligence and Quantum are aligned with Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" and Executive Order 13859 "Maintaining American Leadership in Artificial Intelligence." We coordinate this with the Secretary's Artificial Intelligence program to ensure broadest awareness and surface new opportunities. For example, the Cyber Attack Detection and Accommodation for Energy Delivery Systems project has advanced artificial intelligence technology by developing a commercially viable, field demonstrated, self-learning and resilient cyber-attack/anomaly automatic detection and accommodation technology to provide uninterrupted, equipment safe, controlled power generation to the grid even in the presence of attacks. This project is integral to the defense-in-depth strategy to support improved resilience in the national critical energy infrastructure. The Cyber Attack Detection and Accommodation for Energy Delivery project uses feature-based machine learning and control and estimation algorithms to detect, localize and mitigate attacks in real-time with very low false positive rates with multiple heterogeneous data streams.

To advance technologies in quantum computing, researchers at Los Alamos National Laboratory (LANL) have developed several technologies based in Quantum Information Science (QIS) for use in improving the security of the nation's electric grid. Specifically, LANL has demonstrated quantum secured communications over existing installed optical fiber infrastructure. This technology allows entities on a network to prove their identity to one another, and to be sure the messages they send are transmitted faithfully. For example, a utility control center can be certain that data received from a substation was indeed sent by that substation and has not been spoofed or altered in transit.

Additionally, CESER's Cybersecurity Risk Comparison tool is developing a method to quantify cyber risk reduction achieved through the deployment of defensive countermeasures, including selected other CEDS R&D-funded tools and technologies. Using the attack tree developed by the NERC-Critical Infrastructure Protection Committee (CIPC) Cyber Attack Task Force (CATF) and the MITRE ATT&CK framework, the research effort will develop a methodology to quantify the dollar investment associated with reducing the number of cyber attack tree paths that are functionally available to the adversary. It will achieve this through deployment of selected countermeasures, and by comparing it to the number of attack tree paths without deployment of the same countermeasures, for a specified control system architecture.

For example, the Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF) project is designed to anticipate the impact a command will have on a control system environment. If any commands would result in damage to the system or have other negative consequences, CODEF will have the ability to prevent their execution. This type of solution is especially intriguing as it can detect malicious activity regardless of the source, be it an insider threat or an external actor.

Strengthening our Workforce Development

The final area I would like to highlight is one that is truly foundational in nature, cybersecurity workforce development. It is also a national priority outlined in the President's National Cyber Strategy, and further reinforced by Executive Order 13870, "America's Cybersecurity Workforce." Through our SLTT workforce development efforts through organizations like the National Association of State Energy Officials (NASEO), we are developing a multifaceted approach including online trainings, playbooks, workshops, and guidance. This builds capacity throughout the sector and guarantees that the State energy officials we engage with regularly have the necessary and current skills and resources needed to prepare for and respond to energy disruptions of significance, including cyber emergencies.

Building a culture of cybersecurity throughout the energy sector is critical. Technology is playing an increasingly significant role in the energy sector, requiring a workforce with knowledge of both cybersecurity and power systems. Further encouraged by the President's Executive Order on America's Cybersecurity Workforce, DOE is working in conjunction with National Rural Electric Cooperative Association (NRECA) and the American Public Power Association (APPA) to help further enhance the culture of security within their utility members' organizations. With more than a quarter of the Nation's electricity customers served by municipal public power providers and rural electric cooperatives, it is critical that they have the tools and resources needed to address security challenges. To address risks and manage the risks to an acceptable level, APPA and NRECA are developing security tools, educational resources, updated guidelines, and training on common strategies that can be used by their members to improve their cyber and physical security postures. Exercises, utility site assessments, and a comprehensive range of information sharing with their members will all be used to bolster their security capabilities.

DOE is also continuing and expanding our annual collegiate-level cyber defense competition. In 2018, DOE held two competitions to help develop the next generation of cybersecurity professionals to help secure our Nation's critical energy infrastructure. DOE's Cyber Defense Competition (CDC) took place in April, with 25 college and university teams competing at three National Laboratories. In December 2018, DOE hosted the CyberForce Competition™, with 64 college and university teams from 24 states and Puerto Rico competing at seven National Laboratories. The next CyberForce Competition™ will take place in November 2019 at ten National Laboratories, and is expected to expand beyond the collegiate level.

Additionally, CESER is working in coordination with the Office of Management and Budget (OMB), the Office of Personnel Management (OPM) and the Federal Chief Information Officer (CIO) Council, to fully leverage current hiring authorities under the Cybersecurity Enhancement Act of 2014. We intend to do this, in part, by utilizing cyber competitions announcements as preliminary job announcements, and then proceed through competition scores to identify highly qualified cyber professionals for potential placement and retention into the Federal Government.

Conclusion

Reliable and resilient energy infrastructure is critical to U.S. economic competitiveness, innovation, and leadership. Establishing CESER is the result of the Administration's commitment to and prioritization of energy security and national security. CESER is working on many fronts collaborating with industry and State and local governments to protect our Nation's critical electrical infrastructure from all hazards, including this growing cyber threat. Our long-term approach will strengthen our national security and positively impact our economy.

I appreciate the opportunity to appear before this Subcommittee to discuss cybersecurity in the energy sector, and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address physical and cybersecurity challenges to the grid.

Honorable Karen S. Evans

Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

Karen S. Evans was sworn in by U.S. Deputy Secretary of Energy Dan Brouillette as the Assistant Secretary for the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) on September 4, 2018. Mrs. Evans was confirmed as Assistant Secretary for CESER by the U.S. Senate on August 28, 2018.

Before being nominated by President Donald J. Trump to lead the Department of Energy's cybersecurity efforts, Mrs. Evans was the National Director of the U.S. Cyber Challenge, a public-private program designed to help address the skills gap in the cybersecurity field. She also served as an independent director and outside manager for publicly-traded companies.

Mrs. Evans was previously a top IT official at the Office of Management and Budget under President George W. Bush in the position that is now known as the Federal CIO and also served as the Department of Energy's Chief Information Officer.

She received her MBA and BA in Chemistry from West Virginia University.