Written Testimony of Assistant Secretary Bruce J. Walker

Office of Electricity Delivery and Energy Reliability

U.S. Department of Energy

Before the

U.S. House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

December 8, 2017

Introduction

Chairman Harper, Ranking Member DeGette, and distinguished Members of the Subcommittee, thank you for the opportunity to discuss the continuing cybersecurity threats facing our national energy infrastructure and the Department of Energy's (DOE's) role in protecting the Nation's critical energy infrastructure from this hazard. Cybersecurity and the resilience of the energy sector are top priorities of the Secretary and a major focus of the Department.

Our economy, national security, and even the well-being of our citizens depend on the reliable delivery of electricity. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve the resiliency of energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary of Energy and DOE are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure from physical security events, natural and man-made disasters, and cybersecurity threats.

The Unique Nature of Energy Sector Cybersecurity

Cyberattacks targeting "information technology," or IT, including computing and business applications, to cause disruptions, obtain access to email accounts and personal information, exfiltrate data to release to the world at large, and exploit information for private gain are growing increasingly common. The energy sector is not immune to such attacks.

However, our adversaries understand that the energy sector is a valuable target not because of its IT systems, but because of the assets that the sector controls. Accordingly, we have seen an increased interest in vulnerabilities of the "operating technology," or OT, of energy delivery systems and other critical infrastructure as well. OT systems consist of industrial control

systems (or ICS), programmable logic controls, and their associated supervisory control and data acquisition software (known as SCADA). The heavy use of OT systems has made electric utilities, oil and natural gas providers, hydro and nuclear facilities, and water utilities prime targets for OT-related cyber-attacks. The disruption of any one of these is not only inherently problematic, it also hampers the ability to respond to any type of emergency event.

The Department's focus on OT systems specific to the energy sector makes our activities both distinct from, and complementary to, the activities of the Department of Homeland Security (DHS) and our other Federal agency partners. The cybersecurity of energy sector OT systems requires specific and focused attention because of their need for extremely high reliability and availability, the fact that any significant reduction in the speed of the systems is unacceptable, and because these systems are so critical to underpinning the Nation's economic health, public safety, and national security.

In December 2015, the first known successful cyber-attack on power grid OT took place in Ukraine. Over 225,000 residents were left without power for several hours in the coordinated attack, and a second attack occurred in December 2016 that left portions of Kiev without electricity. More recently, publicly-available information about threats such as the Crash Override malware used in Ukraine and the nation-state activities described under the name "Dragonfly 2.0" are just two of many examples that illustrate the threat to the Nation's energy infrastructure is real and growing more concerning by the day.

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and response to, cybersecurity threats, the Federal government's operational framework is provided by Presidential Policy Directive 41 (PPD-41). A primary purpose of PPD-41 is to clarify the roles and responsibilities of the Federal Government during a "significant cyber incident," which is described as a cyber incident that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Under the PPD-41 framework, DOE works jointly with other agencies and private sector organizations, including the Federal government's designated lead agencies for coordinating the response to significant cyber incidents by protecting assets and countering threats: 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 the National Cyber Investigative Joint Task Force, respectively. In the event of a cybersecurity emergency in the energy sector, closely aligning DOE's activities with those of our partners at DHS and DOJ ensures DOE's deep expertise with the sector is appropriately leveraged.

DOE's role in energy sector cybersecurity was codified by Congress through the Fixing America's Surface Transportation (FAST) Act. That legislation designated DOE as the Sector Specific Agency (or SSA) for cybersecurity of the energy sector. In extreme cases, the

Department can use its legal authorities such as those in the Federal Power Act, as amended by the FAST Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. The Secretary of Energy was provided a new authority, upon declaration of a "Grid Security Emergency" by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to respond as needed to the threat of cyber and physical attacks on the grid. The Grid Security Emergency authority is unique to DOE and an important element in partnering with DHS and DOJ to fully address the cybersecurity risks to the energy sector.

In addition, DOE serves as the lead agency for Emergency Support Function 12 (ESF-12) under the National Response Framework. As the lead for ESF-12, DOE is responsible for facilitating the restoration of damaged energy infrastructure. The Department works with industry and Federal, state, and local partners to facilitate response and recovery. Combining DOE roles as the SSA in cybersecurity with national response ensures incidents with both cyber and physical impacts can be coordinated for the energy sector.

Importance of Partnerships

Before I describe the details of the Department's activities in support of the energy sector's cybersecurity, I must first focus on the most foundational aspect of our activities: partnerships. The Federal government does not own or operate the vast majority of the assets in the Nation's energy sector, nor does DOE hold a monopoly on protecting the Nation's critical infrastructure from cyber threats. As such, strong partnerships throughout the public and private sectors and with our Federal colleagues at DHS and other law enforcement and national security-oriented agencies are essential to function effectively.

DOE has collaborated with the energy sector for nearly two decades in voluntary public-private partnerships that engage energy owners and operators at all levels – technical, operational, and executive – along with state and local governments, to identify and mitigate cyber and physical risks to energy systems.

These partnerships are built on a foundation of earned trust that promotes the mutual exchange of information and resources to improve the security and resilience of critical energy infrastructures. These relationships acknowledge the special security challenges of energy delivery systems and leverage the distinct technical expertise within industry and government to develop solutions.

The security, integrity, and resiliency of the energy infrastructure is both a state and Federal government concern because energy underpins the operations of every other type of critical infrastructure, the economy, and public health and safety. The owners and operators of energy infrastructure, however, have the primary responsibility for the full spectrum of cybersecurity risk management: identify assets, protect critical systems, detect incidents, respond to incidents, and recover to normal operations.

When the lights go out or gasoline stops flowing in pipelines, the first responder is usually not the state or Federal Government but, rather, industry or local government. This is why public-private partnerships regarding cybersecurity are paramount – they recognize the distinct roles and capabilities of industry and government in managing our critical energy infrastructure risks.

In the Energy Sector, the core of critical infrastructure partners consists of the Electricity Subsector Coordinating Council (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 co-chaired with 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're working together in a whole-of-government response.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or "SCCs" are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council (CIPAC) 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 Strategy for the Energy Sector

DOE plays a critical role in supporting energy sector cybersecurity to enhance 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 what I call an ecosystem of resilience: a network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover.

As part of a comprehensive energy cybersecurity resilience strategy, the Department is focusing cyber support efforts to enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness and planning across local, state, and Federal levels; and leverage the expertise of DOE's National Labs to drive cybersecurity innovation.

Enhance visibility and situational awareness of operational networks

It is necessary for partners in the energy sector and the government to share emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber-attacks more rapidly. An example of this type of collaboration is the Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public-private partnership that is primarily funded by industry,

administered by the Electricity Information Sharing and Analysis Center (E-ISAC), and enhanced by DOE through intelligence analysis by DOE's Office of Intelligence and Counterintelligence.

The purpose of CRISP is to share information among electricity subsector partners, DOE, and the Intelligence Community to facilitate the timely bi-directional sharing of unclassified and classified threat information to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the Intelligence Community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 75 percent of the total number of continental United States electricity customers.

If CRISP has demonstrated one finding to DOE, the E-ISAC, and our industry partners, it is that continuous monitoring of critical networks and shared situational awareness is of utmost importance in protecting against malicious cyber activities. Programs such as CRISP are critical for facilitating the identification of and response to advanced persistent threats targeting the energy sector.

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of taking the lessons learned from CRISP and developing an analogous capability to monitor traffic on OT networks via the Cybersecurity for the Operational Technology Environment (CYOTE) pilot project. Observing anomalous traffic on networks – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack in its early stages.

Increase alignment of cyber preparedness and planning across local, state, and Federal levels

As the Energy SSA, DOE works at many levels of the electricity, petroleum, and natural gas industries. 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.

Earlier this year, DOE-OE and the National Association of Regulatory Utility Commissioners (NARUC) released the third edition of a cybersecurity primer for regulatory utility commissioners. The updated primer provides best practices, access to industry and national standards, and clearly-written reference materials for state commissions in their engagements with utilities to ensure their systems are resilient to cyber threats. This document is publicly available on the NARUC Research Lab website, benefitting not only regulators, but state officials as well.

We are continuing to work with the NARUC Research Lab to support regional trainings on cybersecurity throughout the year, with the goal of building commissioner and commission staff

expertise on cybersecurity so they ensure cyber investments are both resilient and economically sound.

DOE also continues to work closely with our public and private partners so our response and recovery capabilities fully support and bolster the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the SCCs to synchronize DOE and industry cyber incident response playbooks.

DOE-OE also engages directly with our public and private sector stakeholders to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. Innovation and preparedness are vital to grid resilience. In December 2016, DOE and the National Association of State Energy Officials (NASEO) co-hosted the Liberty Eclipse Exercise in Newport, Rhode Island, which focused on a hypothetical cyber incident that cascaded into the physical world, resulting in power outages and damage to oil and natural gas infrastructure. The event featured 96 participants from 13 states, and included representatives from state energy offices, emergency management departments, utility commissions, as well as Federal partners, such as FEMA, and private sector utilities and petroleum companies.

And just last month, DOE participated in GridEx IV, a biennial exercise led by the North American Electric Reliability Corporation (NERC) that was designed to simulate a cyber and physical attack on electric and other critical infrastructures across North America. This and other similar large scale exercises continue to highlight the interdependencies between our Nation's energy infrastructure and other sectors.

While the after-action report has yet to be released, during GridEx IV, it was clear that collaboration between industry and the Federal Government has strengthened greatly since Superstorm Sandy and GridEx III. The executed coordination in response to this year's hurricane season also is evidence of this strengthening.

Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinate 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 that we continue working with our industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary's authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.

Continued coordination with Federal and industry partners and participation in preparedness activities like GridEx enables DOE to identify gaps and develop capabilities to support cyber response as the SSA.

Leverage the expertise of DOE's National Laboratories to drive cybersecurity innovation

Beyond providing guidance and technical support to the energy sector, DOE-OE also supports a R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy

systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control and OT systems is much different than that of typical IT systems. 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 be difficult.

DOE-OE's Cybersecurity for Energy Delivery Systems (CEDS) R&D program is designed to assist the energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. DOE-OE co-funds industry-led, National Laboratory-led, and university-led projects with 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 (S&T).

To select cybersecurity R&D projects, DOE constantly examines today's threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects. For example, the Artificial Diversity and Defense Security (ADDSec) project will develop solutions to protect control system networks by constantly changing a network's virtual configuration, much like military communications systems that rapidly change frequencies to avoid interception and jamming. As a result, ADDSec can harden networks against the mapping and reconnaissance activities that are the typical precursors to a cyberattack.

Another project, the Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF), is designed to anticipate the impact a command will have on a control system environment. If the commands would result in damage to the system or 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.

DOE is also working in conjunction with the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) 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 they have the tools and resources needed to address security challenges. 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.

Conclusion

Threats continue to evolve, and DOE is working diligently to stay ahead of the curve. The solution is an ecosystem of resilience that works in partnership with local, state, and industry stakeholders to help provide the methods, strategies, and tools needed to help protect local communities through increased resilience and flexibility. To accomplish this, we must accelerate information sharing to inform better local investment decisions, encourage innovation and the use of best practices to help raise the energy sector's security maturity, and strengthen local incident response and recovery capabilities, especially through participation in training programs and preparedness exercises.

Building an ecosystem of resilience is – by definition – a shared endeavor, and keeping a focus on partnerships remains an imperative. DOE is committed to continue building on its years of coordinating with and fostering vital energy sector relationships with our Federal partners, as well as investing in technologies to enhance security and resilience in order to support industry efforts to respond to, and recover quickly from, all threats and hazards.

I appreciate the opportunity to appear before the Subcommittee to discuss the cybersecurity of the energy sector. I would, however, be remiss if I did not take a moment to stress that the interdependent nature of our infrastructure requires that all sectors be constantly focused on improving their cybersecurity posture. Collaboration among DOE, DHS, and the rest of the Federal family is absolutely critical to ensuring that we remain both ahead of the curve and resilient to any potential cyberattack. DOE, as always, looks forward to our continued partnership to share best practices, collaborating where appropriate and possible, and helping to protect our civilian infrastructure from the Nation's cyber adversaries.