U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

December 6, 2017

TO: Members, Subcommittee on Oversight and Investigations

FROM: Committee Majority Staff

RE: Hearing entitled "Examining the Role of the Department of Energy in Energy Sector Cybersecurity"

I. INTRODUCTION

The Subcommittee on Oversight and Investigations will hold a hearing on Friday, December 8, 2017, at 9:00 a.m. in 2123 Rayburn House Office Building. The hearing is entitled "Examining the Role of the Department of Energy in Energy Sector Cybersecurity." The hearing will examine the Department of Energy's roles and responsibilities for cybersecurity in the energy sector and the department's current and future efforts to assist the sector with this growing threat.

II. WITNESSES

- **Bruce Walker**, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy.

III. BACKGROUND

A. The Challenge of Cybersecurity

Cybersecurity is a broad, dynamic, and rapidly evolving challenge for modern society. As we become more dependent on the Internet and information technologies, cyber threats will continue to proliferate at an exponential rate and the consequences of incidents will become increasingly profound. The evolution of cyber-physical systems such as cars, medical devices, the electric grid, and other connected consumer products not only increase the attack surface, but also escalate the threat from loss of information to potential physical harm.

Given the scope and scale of society's dependence on connected technologies and the attendant cyber threat, cybersecurity is not something that can be "solved." As the threats proliferate and consequences become more severe, the nation must strengthen its approach to cybersecurity. The challenge lies in the fact that there is no single solution to better cybersecurity; it depends on multiple improvements, new approaches, and fresh thinking, as well as a commitment to strengthening existing institutions. All this depends on trust, coordination, and engagement between government and private sector partners.

B. Public-Private Partnerships in Critical Infrastructure

Engagement between public and private sector partners is an important part of any security challenge, including cybersecurity. When it comes to the protection of our critical infrastructure, however, public-private partnerships are vital. Critical infrastructures are "the essential services that underpin American society and serve as the backbone of our nation's economy, security and health."[1] Given the importance of these assets to our society, the public sector's responsibility for safety and security depends on a strong relationship with private sector partners that own and operate approximately 85 percent of the nation's critical infrastructure.[2] The success of these public-private partnerships depends on trust, leadership, and commitment from both sides.

To facilitate this relationship, the United States relies on a public-private partnership model that has evolved over the last two decades.[3] In this model, the private sector is split into 16 critical infrastructure sectors, each of which relies on four organizations either identified or created within the model – a Sector Specific Agency (SSA), a Government Coordinating Council (GCC), a Sector Coordinating Council (SCC), and an Information Sharing and Analysis Center (ISAC). Each of these organizations plays a unique and complimentary role in helping to shape and guide cybersecurity efforts throughout the sector.

- **Sector Specific Agencies:** For each sector, SSAs serve as the leader of federal engagement, communication, and collaboration with private sector partners. This includes representing and advocating for their sector's unique equities, providing support and guidance to their industry stakeholders, and implementing government-wide cybersecurity initiatives and strategies.[4]

- **Government Coordinating Councils:** Led by a sector's SSA, GCCs bring together government stakeholders from federal, state, local, territorial, and tribal agencies to help coordinate and deconflict government efforts.

- **Sector Coordinating Councils:** Comprised of industry stakeholders from across the sector, SCCs are tasked with representing industry equities and needs, guiding and coordinating efforts among industry to address issues, and working with their designated SSA and GCC to help implement initiatives and mandates.

[1] U.S. Dep't of Homeland Security, *Sector-Specific Agencies*, https://www.dhs.gov/sector-specific-agencies (last visited Dec. 5, 2017).
[2] Office of the Director of National Intelligence, Partner Engagement, *Critical Infrastructure and Key Resources*, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources (last visited Dec. 5, 2017).
[3] Over the course of the last two decades, the executive branch has issued a series of documents that either established or refined this model, including: Homeland Security Presidential Directive (HSD-7), Presidential Policy Directive 21 (PPD-21), and PPD-41. These in turn led to the design and implementation of the National Infrastructure Protection Plan (NIPP) and the National Cyber Incident Response Plan (NCIRP).
[4] *Id.*

- **Information Sharing and Analysis Centers:** ISACs are meant to improve the cybersecurity of industries through the establishment of organizations whose primary purpose is to collect, analyze, and disseminate cybersecurity threat information. This information then may be shared among stakeholders

C. Public-Private Partnership in the Energy Sector

The Energy Sector is arguably the most critical infrastructure sector. Almost every aspect of daily lives depends on reliable energy – it powers our transportation, homes, and businesses, facilitates communications, and contributes to health care. As a result, Presidential Policy Directive 21 identifies the energy sector as "uniquely critical" due to the "enabling functions" it provides across all critical infrastructure sectors.[5] .

Under the current public-private partnership model, the Department of Energy (DOE) serves as the SSA for the Energy Sector. The Energy Sector is comprised of three interrelated subsectors – electricity, oil, and natural gas. This includes "the production, refining, storage and distribution of oil gas and electric power[.]"[6] There are, however, a few exclusions under the current structure including, "hydroelectric and commercial nuclear power facilities and pipelines.[7]

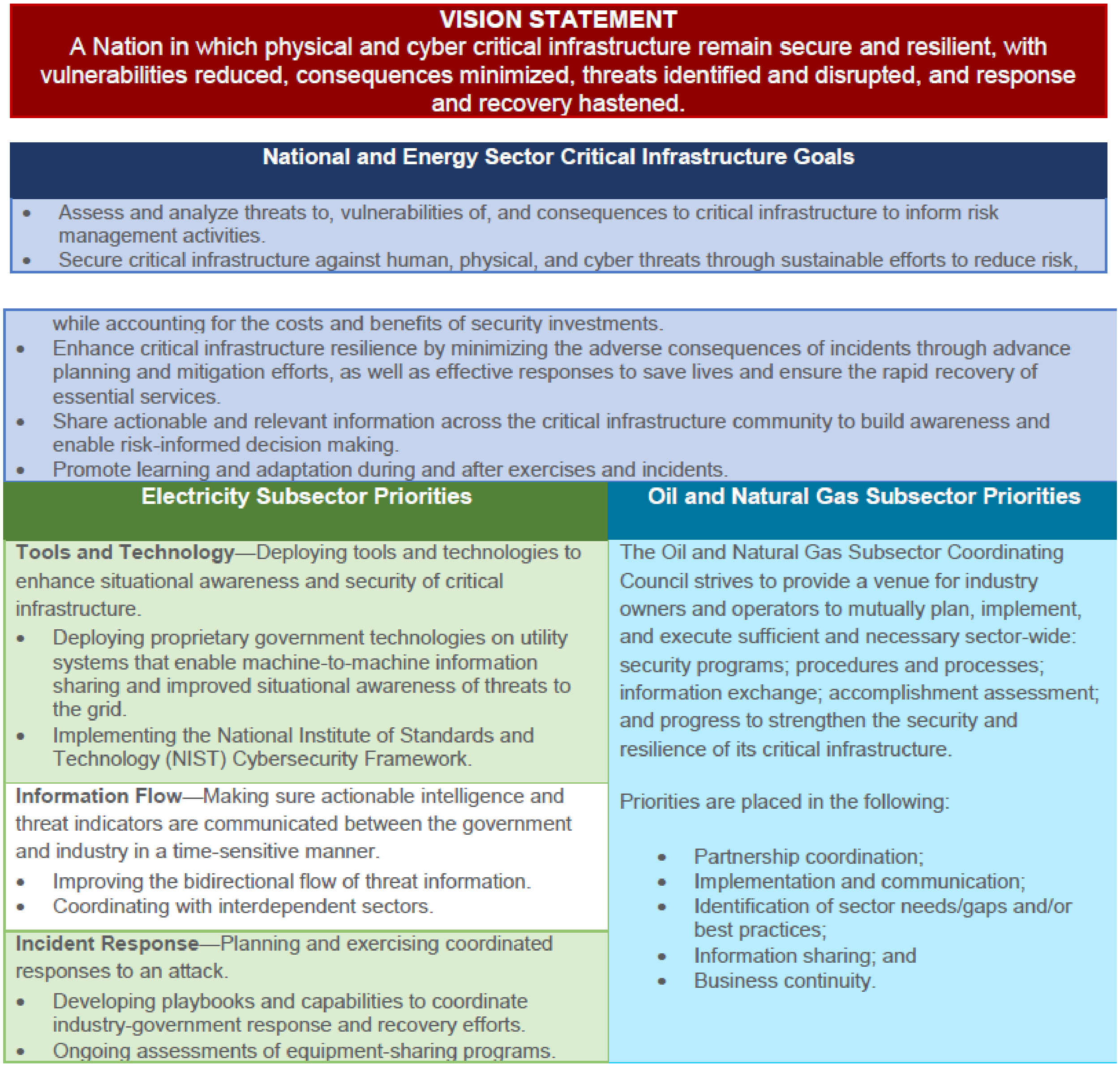
Private sector engagement with DOE, as the SSA, and other government partners through the GCC, is led by two subsector coordinating councils – Electricity and Oil and Natural Gas. The sector is guided by mutually accepted "national goals," as well as subsector priorities, which contribute to national goals (see Table 1).

[5] The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience (February 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[6] U.S. Dept. of Energy and U.S. Dept. of Homeland Sec., *Energy Sector-Specific Plan* (2015), https://www.dhs.gov/publication/nipp-ssp-energy-2015, at 3.

[7] *Id.*

Table 1 – National Goals and Subsector Priorities for the Energy Sector[8]



VISION STATEMENT

A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.

National and Energy Sector Critical Infrastructure Goals

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities.
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments.
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services.
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making.
- Promote learning and adaptation during and after exercises and incidents.

Electricity Subsector Priorities	Oil and Natural Gas Subsector Priorities
Tools and Technology—Deploying tools and technologies to enhance situational awareness and security of critical infrastructure. • Deploying proprietary government technologies on utility systems that enable machine-to-machine information sharing and improved situational awareness of threats to the grid. • Implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework.	The Oil and Natural Gas Subsector Coordinating Council strives to provide a venue for industry owners and operators to mutually plan, implement, and execute sufficient and necessary sector-wide: security programs; procedures and processes; information exchange; accomplishment assessment; and progress to strengthen the security and resilience of its critical infrastructure. Priorities are placed in the following: • Partnership coordination; • Implementation and communication; • Identification of sector needs/gaps and/or best practices; • Information sharing; and • Business continuity.
Information Flow—Making sure actionable intelligence and threat indicators are communicated between the government and industry in a time-sensitive manner. • Improving the bidirectional flow of threat information. • Coordinating with interdependent sectors.	
Incident Response—Planning and exercising coordinated responses to an attack. • Developing playbooks and capabilities to coordinate industry-government response and recovery efforts. • Ongoing assessments of equipment-sharing programs.	

In recent years, DOE has done a commendable job as the SSA for the energy sector, especially with the electricity subsector. Through executive-level engagement and commitment, both from the Department and industry partners, the subsector has developed significant trust, collaboration, and unity of message between public and private partners. DOE’s leadership has increased participation and focus across the sector, which has contributed to the enhancement of important partnerships and programs, such as the collection and sharing of information.

[8] *Id.* at 3-4.

One notable example facilitated by this partnership between DOE and the electricity subsector is the Cybersecurity Risk Information Sharing Program (CRISP). Born out of research at the national labs, CRISP has evolved into a robust public-private partnership, co-funded by DOE and industry and managed by the Electricity Information Sharing and Analysis Center (E-ISAC). Through the use of DOE developed sensors and threat analysis techniques – as well as the Department's participation in the Intelligence Community – CRISP enables "the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources."[9] CRISP has grown over the years and current participants provide power to over 75 percent of customers in in the continental U.S.[10] The success of this program is encouraging new partnerships and pilot programs, including one that relies on a model that is similar to CRISP, but focuses on the operational technology (OT) environment.[11]

D. Cybersecurity in the Energy Sector

The public-private partnership model provides a foundation for addressing all threats – including but not limited to cyber, physical, human, and weather – relevant to a specific critical infrastructure sector. Threats and their perceived or respective risk vary greatly across and within sectors. As more of our world becomes connected, cyber threats are increasing in prevalence and sophistication, introducing new and complex challenges to critical infrastructure sectors.

As with other sectors, cyber threats are a growing concern in the energy sector. Recent cyber-related events have demonstrated the increased attention on this sector from sophisticated actors, but also the potential risks of a successful attack on U.S. energy systems. For example, in December 2015, cyberattacks on the Ukrainian Power Grid shut off power to approximately 225,000 customers across several regions.[12] While the outages were relatively short-lived, this was the first publicly acknowledged example of a cyber-related power outage. More recently, public reports described efforts by a sophisticated actor to conduct espionage on energy sector targets in the U.S. and internationally.[13] According to researchers, the objectives of this campaign focused on understanding how energy systems operate and potential points of entry to operational systems, presumably for the purpose of disruption or sabotage.

As the energy sector continues to modernize, the cybersecurity challenges become increasingly complex. For example, as the electric grid is increasingly connected – whether

[9] U.S. Dept. of Energy, Office of Electricity Delivery and Energy Reliability, *Energy Sector Cybersecurity Preparedness*, https://energy.gov/oe/energy-sector-cybersecurity-preparedness-0 (last accessed Dec. 5, 2017).
[10] *Id.*
[11] *Id.*
[12] The Ukraine incidents affected 225,000 customers and lasted for several hours in three service territories, which was considered comparatively low impact in terms of overall power system impacts, according to *Analysis of the Cyber Attack on the Ukrainian Power Grid*, by SANS ICS, March 18, 2016. See www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[13] Symantec, "Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group" (October 20, 2017) *available at* https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.

through smart grid technologies or interaction with consumer devices and distributed energy resources – it becomes more of a platform than commodity distribution service. While this provides tremendous opportunity for innovation, efficiency, and resiliency, it also expands the attack surface, introducing new vulnerabilities and potentially opening the door to wider range of threat actors. .

Congress, government agencies, and the private sector have taken steps to address current and future cyber risks. These steps include establishing mandatory nationwide reliability standards,[14] leveraging public-private partnerships to improve trust and information sharing, and providing new authorities to address grid security emergencies.[15]

E. Grid Security Exercise

The Grid Security Exercise (GridEx) is a biennial event conducted by the North American Electric Reliability Corporation (NERC) to test and strengthen utilities' response to coordinated cyber and physical threats to the electric grid. The initial GridEx was held in 2011, with subsequent exercises taking place in 2013 (GridEx II) and 2015 (GridEx III). The fourth exercise – GridEx IV – took place in November of this year.

Prior to each GridEx, NERC engages in an extensive, months-long effort to design the scenario, plan the exercise, and coordinate engagement with stakeholders. These efforts – combined with lessons from prior exercises – not only increase the sophistication of the program, but also encourage greater awareness and participation from stakeholders. For example, in 2011, 76 organizations participated in the first GridEx. In 2015, GridEx III involved more than 4,400

[14] In 2005, Congress acted to establish reliability standards for the electricity sector by passing the Energy Policy Act of 2005, which amended the Federal Power Act (FPA) and authorized the Federal Energy Regulatory Commission (FERC) to create an Electric Reliability Organization (ERO) with the authority to establish and enforce reliability standards. Under this authority, FERC designated NERC as the ERO. NERC is a non-profit international regulatory authority whose mission is to assure the reliability and security of the North American bulk power system. Through an extensive stakeholder process, FERC, NERC, and industry stakeholders have developed and implemented infrastructure protection standards for cybersecurity.

[15] The Fixing America's Surface Transportation (FAST) Act of 2015 updated and expanded the DOE's authorities to counter cybersecurity threats. Specifically, section 61003 amends the FPA and designates the DOE as the lead sector-specific agency for energy sector cybersecurity. These provisions authorize the Secretary of Energy to address grid security emergencies if the President provides a written directive or determination identifying a grid security emergency. The Secretary is authorized to take emergency measures to protect the bulk power system or defend critical infrastructure, including ordering critical electric infrastructure owners and operators to take appropriate actions. The Act defines "Grid Security emergency" as an "occurrence or imminent danger of—a malicious act using electronic communication or an electromagnetic pulse, or a geomagnetic storm event, that could disrupt the operation of those electronic devices or communication networks, including hardware, software, and data, that are essential to the reliability of critical electric infrastructure or of defense critical electric infrastructure."

The FAST Act also facilitates the protection and voluntary sharing of critical infrastructure information between private sector asset owners and the Federal Government. Additionally, the FAST Act exempts designated Critical Electric Infrastructure Information from certain federal and state disclosure laws; requires FERC to facilitate voluntary information sharing among federal, state, local and tribal authorities, the ERO, regional entities, owners, operators, and users of the bulk-power system in the United States; and establishes sanctions for the unauthorized disclosure of shared information.

individuals from 376 organizations across North America – including industry, law enforcement, and government agencies.[16]

The actual exercise, led by NERC's E-ISAC, occurs over two days and involves two primary components: a distributed play exercise and an executive tabletop (See Figure 1).[17]

- Distributed Play Exercise – This portion of GridEx is the execution of the scenario designed by NERC. Over two days, NERC engages participants across the country with scenario events called injects.[18] This enables industry to test their operational response as well as the effectiveness of internal and external communications.

- Executive Tabletop – On the second day, industry executives and government leaders gather to discuss the "policy issues, decisions, and actions needed to respond to a major grid disruption caused by simulated physical and cyber attacks."[19]

Lessons learned from the exercises are used to develop mitigating strategies to improve response, communication, and leadership across the sector.

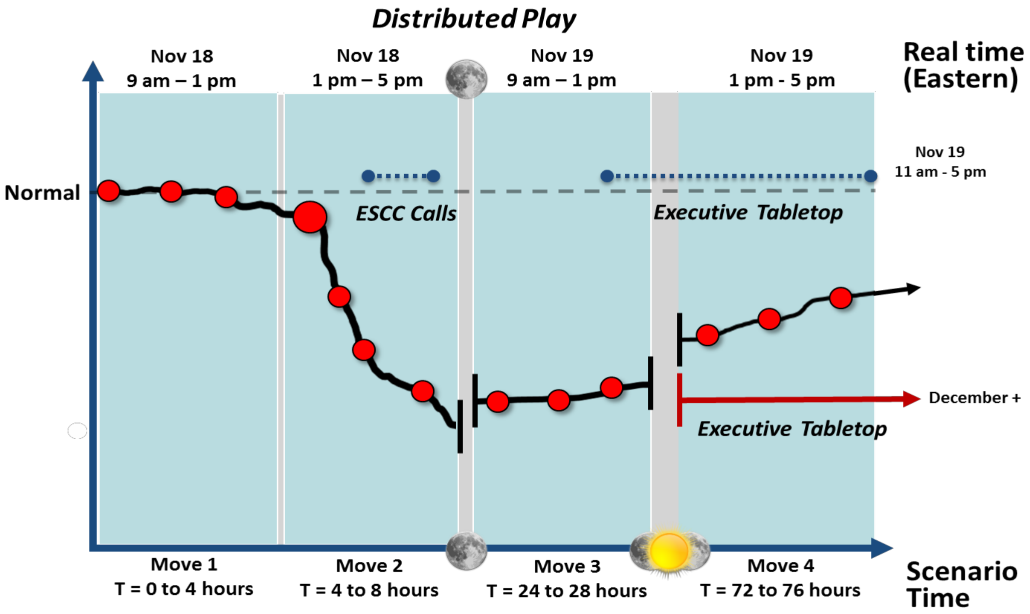
[16] North American Electric Reliability Corporation, *Grid Security Exercise: GridEx III Report* (March 2016) *available at* http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf, at 1 (hereinafter *GridEx III Report*).

[17] *Id.* at 7.

[18] North American Electric Reliability Corporation, "GridEx IV Fact Sheet," *available at* http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx.

[19] *GridEx III Report*, supra note 15, at v.

Figure 1. An illustration of impacts on the grid, as well as interplay and sequencing of exercise components, based on the scenario utilized in GridEx III.



IV. ISSUES

The following issues may be explored at the hearing:

- How has DOE helped the electricity subsector interact with other portions of the energy sector?
- How does DOE intend to build on past experience to improve or expand its contributions to cybersecurity in the energy sector?
- Are there gaps or weaknesses in the energy sector's approach to cybersecurity, and how does DOE intend to address those issues?
- How has DOE helped the national lab system improve cybersecurity in the energy sector?
- How do the results of GridEx IV inform the sector's approach to cybersecurity?

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact John Ohly or Brighton Haslett of the Committee staff at (202) 225-2927.