The Secretary of Energy
Washington, DC 20585

March 13, 2018

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter requesting input to assess the quality of coordination among the various Federal entities relating to cybersecurity of the Nation's pipeline system. The Department of Energy (DOE) is providing the attached response to your questions.

America's energy supply is essential to our national and economic security. DOE has a vital role in protecting that supply, and I have no higher priority. DOE serves as the Sector Specific Agency for Energy under Presidential Policy Directive 21 and the lead Federal agency for Emergency Support Function (ESF) #12 – Energy under the National Response Framework. As such, I am in the process of establishing the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to elevate these issues commensurate with the seriousness of the threat. This will better position the Department to continue working closely with industry partners, the Department of Homeland Security, the Department of Transportation, and the Federal Energy Regulatory Commission regarding pipeline security and safety initiatives as they relate to resilience and reliability.

I am pleased to report that DOE and DHS provided a briefing to Committee staff on pipeline cybersecurity issues on March 12, 2018 and we are working with the staff to arrange for a more detailed briefing on federal threat assessments concerning pipeline infrastructure. As you consider cybersecurity issues around the oil and natural gas pipeline network, DOE would like to emphasize the connected nature of our energy system as a feedstock to electric generation facilities, fuel assurance, and overall resilience.

Thank you again for your attention to this important subject. If you have any additional questions, please do not hesitate to contact me or Mr. Marty Dannenfelser, Deputy Assistant Secretary for House Affairs, Office of Congressional and Intergovernmental Affairs, at (202) 586-5450.

Sincerely,

Rick Perry

Rick Perry

Enclosure

RESPONSE TO HOUSE ENERGY AND COMMERCE LETTER TO SECRETARY PERRY REGARDING PIPELINE CYBERSECURITY

Question 1: Describe the coordination conducted by DOE with DHS, TSA, DOT, FERC, and any other relevant Federal and State agencies as it relates to cybersecurity of pipeline systems.

As the Nation's top 100 pipelines alone supply nearly 84 percent of the Nation's energy[1], pipelines represent a critical part of North America's energy backbone. A coordinated government approach to the cyber and physical security of pipelines, led by the Department of Energy, is essential to ensuring the safe and reliable flow of energy across the U.S.

As the sector-specific agency for the energy sector, DOE works closely with relevant government agencies and oil and natural gas subsector partners on security and resilience including cybersecurity through mechanisms such as through the Oil and Natural gas Sector Coordinating Council and the Energy Government Coordinating Council. As part of the transportation sector, DHS and the Department of Transportation are the co-lead sector-specific agencies for pipeline cybersecurity. DOE works with the Department of Homeland Security (DHS) National Protection and Programs Directorate, the Transportation Security Administration, the U.S. Coast Guard, the Department of Transportation Pipeline and Hazardous Materials Safety Administration, and the Federal Energy Regulatory Commission regarding pipeline security and safety initiatives as they relate to resilience and reliability. Similar to the electric sector, physical and cybersecurity of crude and petroleum pipelines and liquefied natural gas facilities are critical.

The center of gravity for this partnership is the Energy Government Coordinating Council (EGCC)[2], which is co-chaired by DOE and DHS. Through the EGCC, DOE convenes groups listed above, as well as others such as the Federal Bureau of Investigation (FBI), Office of the Director of National Intelligence (ODNI), and Natural Resources Canada (NRCan) to foster a shared national homeland security strategy as it relates to energy infrastructure. This venue provides a useful coordination mechanism to synchronize various collaborations among relevant Federal agencies.

Question 2: Describe the collaboration conducted with owners and operators of pipeline systems, including the relevant subsector coordinating councils and Information Sharing and Analysis Centers (ISACs).

The oil and natural gas (ONG) subsector is a complex system comprised of different segments, including exploration/production, transmission/midstream, and distribution. The protection and resilience of critical ONG infrastructure requires a strong partnership between industry and the Federal Government. The Oil and Natural Gas Sector Coordinating Council (ONG SCC) serves

---

[1] https://www.tsa.gov/news/releases/2016/07/11/securing-and-protecting-our-nations-pipelines

[2] https://www.dhs.gov/sites/default/files/publications/Energy-GCC-Charter-2014-508.pdf

as the industry counterpart to the EGCC and represents the interests of the complex ONG system – including pipelines.

Proactive collaboration between DOE and the ONG SCC strengthens the development of ONG security strategies, activities, policy, and communication across the energy sector as well as across the ONG subsector to support the Nation's homeland security mission. The ONG SCC is comprised of ONG owners and operators from 23 trade associations, representing a broad industry-wide network across the United States and Canada from all business units – drilling, exploration, production, processing, refining, service and supply, transmission, distribution, and transportation (including pipeline, marine, motor, and rail). As a key part of the energy sector, the Pipelines Sector Coordinating Council serves a dual function as the ONG SCC's Pipeline Working Group.

DOE facilitates three principal-level meetings between the EGCC and ONG SCC each year to discuss strategies and high-level vision for the public-private partnership. Specific physical and cybersecurity as well as resilience projects and initiatives are identified during each of these meetings, and DOE works with the ONG SCC and other partners where appropriate to carry out these activities.

In addition to regular coordination through the ONG SCC, DOE Office of Electricity Delivery and Energy Reliability (OE) has engaged the energy sector ISACs, including the ONG ISAC and the Downstream Natural Gas (DNG) ISAC. Recognizing the need for improved information sharing both between industry and government and across the energy sector, DOE convenes monthly meetings with the ONG ISAC, DNG ISAC, and Electricity ISAC to share and discuss cyber threat trends in a classified setting.

Should a major event occur, DOE will actively engage with the sector to support a safe and timely response. In carrying out DOE's Emergency Support Function (ESF) #12 and Sector-Specific Agency responsibilities, DOE holds regular coordination calls with the ONG SCC and Electricity Subsector Coordinating Council (ESCC) to ensure shared situational awareness and to identify any unmet needs. Additionally, DOE's energy response team leverages the Energy Information Administration's (EIA) subject matter expertise to increase awareness and analyze the regional and national impacts of actual or potential supply chain disruptions. The coordination between EIA and DOE was identified in the National Petroleum Council's 2014 study on industry and government's storm preparation, response, and recovery activities, and DOE's broad coordination role was further codified in the Fixing America's Surface Transportation (FAST) Act of 2015. Collectively, these activities and DOE's other response efforts ensure that the interagency and the Nation's SLTT governments respond to major events effecting the energy sector in a coordinated and appropriate manner.

DOE has also been working with the oil and gas sector for over 10 years to develop advanced technologies to better protect the Nation's energy infrastructure against malicious cyber activity. To coordinate public and private activities and investments, DOE partnered with the energy sector in 2006 and again in 2011 to develop a roadmap and common vision to design, install, operate, and maintain resilient control systems that can survive a cyber incident while sustaining

critical functions. The oil and gas sector played a key role in developing these strategic documents serving on the Executive Steering Committees to ensure the roadmaps fully addressed the industry's major cybersecurity challenges, priorities, and technology gaps. Oil and gas sector representatives included API, AGA, INGAA, BP, Chevron, and El Paso.

Question 3: Describe and provide memoranda of understanding or other agreements between DOE and other agencies that have been developed to ensure full and adequate coverage of pipeline systems relating to federal critical infrastructure responsibilities.

DOE serves as the Sector Specific Agency for Energy under Presidential Policy Directive 21 and the lead Federal agency for Emergency Support Function (ESF) #12 – Energy under the National Response Framework. DOE has established a productive public-private partnership with government partners and the pipeline industry to secure the transport of oil and natural gas. DOE works with the Department of Homeland Security's National Protection and Programs Directorate Office of Infrastructure Protection, DHS's Transportation Security Administration, DHS's United States Coast Guard , DHS's Infrastructure Security Compliance Division, the Department of Transportation's Pipeline and Hazardous Materials Safety Administration and the Federal Energy Regulatory Commission to streamline pipeline security and safety initiatives as they relate to resilience and reliability. Formal agreements have not been necessary to coordinate among agencies lending greater flexibility to adjust to emerging threats as needed. The Energy Government Coordinating Council provides a useful coordination mechanism to synchronize various collaborations among relevant federal agencies.

Question 4: Describe the federal resources, including personnel, applied to pipeline cybersecurity vulnerability assessments and related programs.

DOE-OE leads DOE's efforts to secure the U.S. energy infrastructure against all hazards through cybersecurity research and development and in activities to prepare for, respond to, and recover from major disruptive energy events. In FY 2017, approximately $79.2 million of DOE-OE's resources (combination of program dollars and Federal staff) were dedicated to help achieve this objective. The work performed by OE was done in collaboration with DOE's Office of Intelligence and Counterintelligence, which is responsible for all intelligence and counterintelligence activities throughout DOE, including nearly 30 intelligence and counterintelligence offices nationwide. Given this close connection with the intelligence community, DOE is uniquely postured to provide targeted threat classified and unclassified information to the ONG subsector.

Additionally, DOE's 17 national laboratories represent an unparalleled asset available to DOE. The national labs possess unique instruments and facilities, many of which are found nowhere else in the world. They address large scale, complex research and development challenges with a multidisciplinary approach that places an emphasis on translating basic science to innovation. Several of these labs are leading the development of unique cybersecurity solutions that can be deployed across the pipeline industry to further improve the sector's cyber posture.

Question 5: Describe the number, design, and scope of federal audits or assessments to identify vulnerability and cybersecurity risks in pipeline systems.

In an effort to support ONG companies – including pipelines – in assessing their cybersecurity posture, DOE developed the Cybersecurity Capability Maturity Model (C2M2) in 2012. The model is a tool that may be used by the company to assess the maturity of its cybersecurity program through focusing on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology (OT) assets and the environments in which they operate. With specialized knowledge of the OT cybersecurity environment, DOE ISER is uniquely qualified to support pipeline companies identify and mitigate cybersecurity vulnerabilities through resources like C2M2.

The C2M2 supports the ongoing development and measurement of cybersecurity capabilities within any organization by enabling these organizations to consistently evaluate and benchmark their cybersecurity capabilities, prioritize actions and investments, and support adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The model accomplishes this by providing a common set of industry-vetted cybersecurity practices, grouped into ten domains and arranged according to maturity level.

Pipeline companies and other energy sector organizations can facilitate their own C2M2 assessments, or can turn to other parties to assist them in the one-day facilitations. Private companies as well as industry trade associations, such as the American Gas Association (AGA), have leveraged the model to provide individual assessments to their customers or members, respectively. AGA has additionally sponsored several regional workshops to guide participating natural gas member utilities of all sizes through the model. As the model is designed to allow individual companies or associations to assess their own systems, it is difficult to accurately capture the number of ONG companies, including pipelines, which have undergone a C2M2 assessment.

Several of these companies are now in turn participating in DOE's ongoing efforts to update C2M2 to reflect evolving industry best practices and other updates, including the release of a revised NIST Cybersecurity Framework.

Question 6: Describe DOE's specific activity and programs concerning cybersecurity in pipeline systems.

In addition to the work with the ONG SCC, C2M2, energy sector ISACs, and others previously mentioned, DOE has developed a hands-on workshop for energy sector owners and operators to walk through a simulated cyber-attack on energy control systems. This workshop, called "Cyber Strike," leverages lessons learned from the 2015 and 2016 attacks on Ukraine's electric system to better equip U.S. energy companies with the skills to identify and mitigate similar threats. In 2017, DOE partnered with AGA to deliver a version of this training for over 50 of AGA's natural gas utility representatives. DOE currently has six additional workshops planned for 2018 and is developing additional modules targeted for the ONG audience.

DOE hosts an annual Cyber Defense Competition to address the cybersecurity capability gap. Collegiate student teams engage in interactive, scenario-based events to exercise cybersecurity methods, practices, strategy, policy, and ethics, all focused on the energy sector. The scenario for this year's competition, which takes place on April 6, focuses on the interdependencies between natural gas delivery and electric generation. DOE has engaged with AGA and the Interstate Natural Gas Association of America (INGAA) to facilitate engagement between these talented students and natural gas companies.

DOE also works with the trade associations of the ONG SCC to provide classified threat briefings for cleared sector representatives. Through its ties with the intelligence community, DOE regularly delivers briefings related to emerging cyber and physical threats to energy infrastructure. Additionally, in recognizing the need to explore new ways to improve appropriate access to classified threat information, DOE is conducting a pilot of the Government's Secure Video Teleconference (SVTC) capabilities. This goal of this pilot is to exercise DOE's ability to remotely convene a classified threat briefing for cleared energy sector industry representatives, and reduce the barriers to providing them with the information needed to protect their systems.

Since 2010, DOE has utilized the energy sector cybersecurity roadmaps to guide investments of over $200 million in cost-shared R&D to support the oil and gas sector in building resilient energy control systems. Some major accomplishments include:

Artificial Diversity and Defense Security (ADDSec) – Chevron, Washington Gas Energy Systems and SEL, Inc, partnered with Sandia National Laboratory to develop technologies that allow the traditionally static control system to reconfigure itself unpredictably and thereby impede adversarial reconnaissance by making the control system difficult to map – a critical step toward attack planning. If the adversary does succeed in staging a cyber-attack, the control system can automatically reconfigure to sustain critical functions during the cyber-incident.

Role-Based Access Control (RBAC) - Honeywell developed the RBAC technology for the Experion® Process Knowledge System product suite, an energy delivery control system used extensively within the oil and gas industry. RBAC limits user access to the least needed to perform a given task, which helps reduce the risk of unauthorized access, including inside-threats. This technology accounts for roles that are specific to energy delivery operations, for instance, access required for different operating modes, such as normal, start-up, shut-down, and emergency operations. Partners included Idaho National Laboratory (INL) and the University of Illinois at Urbana-Champaign.

Academic-industry Consortia - DOE partnered with DHS to fund the University of Illinois "Cyber Resilient Energy Delivery Consortium" and the University of Arkansas "Cybersecurity Center for Secure Evolvable Energy Delivery Systems" projects. These multiyear consortiums bring together computer scientists and control system engineers guided by industry advisory boards to develop the foundational science and engineering approaches to enhance oil and gas sector cybersecurity and resiliency.

Vulnerability Analysis of Energy Delivery Control Systems – Idaho National Laboratory conducted test bed assessments of more than seven supervisory control and data acquisition

(SCADA) systems widely used in the energy sector. The resulting report describes common vulnerabilities found in the assessments. The vulnerabilities described in this report were routinely discovered in SCADA assessments using a variety of typical attack methods to manipulate or disrupt system operations. The report was designed to provide recommendations to the SCADA vendor and/or owner to identify and reduce the risk of the associated vulnerabilities in their systems.

Cybersecurity Procurement Language for Energy Delivery Systems - designed to provide baseline cybersecurity procurement language for control systems commonly used in the energy sector including: components of energy delivery systems (e.g., programmable logic controllers, digital relays, or remote terminal units), SCADA systems, and networked energy delivery systems (e.g., a natural gas pumping station). Widespread use of common procurement language can greatly enhance the security of the energy sector supply chain as well as lower life-cycle costs by encouraging vendors to build-in security during the design phase.