Testimony of

Mark A. Engels

Senior Enterprise Security Advisor

Dominion Energy

Committee on Energy and Commerce

Energy Subcommittee

U.S. House of Representatives

"DOE Modernization: Legislation Addressing

Cybersecurity and Emergency Response"

March 14, 2018

Testimony Summary

Input to HR 5174, the "Energy Emergency Leadership Act", and HR 5175, the "Pipeline and LNG Facility Cybersecurity Preparedness Act".

- **HR 5175 Section 2(1) – Policies and Procedures and HR 5174 Section 2 – Functions Assigned to Assistant Secretaries**

  DOE is the SSA for the natural gas commodity, and DHS (in coordination with DOT) is the SSA for the pipeline infrastructure. The fact that natural gas pipelines have two SSAs, comprised of three Federal agencies, (DOE, DHS, and DOT) cannot be understated, especially when it comes to interagency-coordination – in advance of, during, and post-incident operations.

  The key to this coordination is maintaining a productive relationship between the Energy Government Coordinating Council (EGCC), which is co-chaired by DOE's Office of Electricity Delivery and Energy Reliability (OE) and the DHS National Protection and Programs Directorate (NPPD), and the Oil and Natural Gas Sector Coordinating Council (ONGSCC).

  While natural gas pipeline operators have a general idea about how the relevant Federal agencies associated with pipeline security should work together, HR 5175 would ideally encourage clarification on this issue. In HR 5174, Energy Emergency Leadership Act, the addition of paragraph 12 in the Department of Energy Organization Act, provides clarity and direction as well.

A more expedient approach may be to encourage a Memo of Understanding (MOU) between DOE and TSA that outlines roles and responsibilities for dealing with cyber and physical security for the ONG sector. TSA already has an MOU with the DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) which has responsibility for pipeline safety. Depending on the type of event, the TSA/DOT MOU has been critical in helping operators understand which Federal entity is the lead agency.

- **HR 5175 Section 2(2) – Coordinate Response and Recovery**

  The language in HR 5175 referencing DOE's coordination with States may actually add complexity to a system that already has structure. Individual pipeline companies, Dominion Energy included, have longstanding relationships with State emergency response organizations, public utility commissions and law enforcement for all hazard events, such as weather. Having DOE attempt to coordinate cyber and physical security for pipelines that could include all 50 States may not result in the value intended. This is particularly true for natural gas response and recovery, which is organized around time-tested local and regional coordination.

- **HR 5175 Section 2(3) – Develop Advanced Cybersecurity Applications**

  HR 5175 should ensure adequate resources and funding to continue efforts like the Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) as well as hardware and software testing via national labs test-beds. Through these programs vendors, academia, labs and industry get involved and ultimately benefits arise from commercialization of products that meet industry requirements.

- **HR 5175 Section 2(4) – Perform Pilot Demonstrations**

  This section is complementary to Section 2(3) but goes further by directing actual demonstrations of technology.

  Asset owners should be involved in the development of testing criteria to ensure the pilot represents, as close as possible, the real world environment in which the technology is intended to operate.

- **HR 5175 Section 2(5) – Develop Workforce Curricula**

  HR 5175 should encourage more training and workforce development similar to *Cyber Strike,* a hands-on workshop sponsored by the Department of Energy and *ATAC,* a methodical approach, develop by Idaho National Laboratory, to aggregate and evaluate cyber-risk related information. Both have proven beneficial to Dominion Energy.

- **HR 5175 Section 2(6) – Provide Mechanisms to Help Evaluate, Prioritize and Improve**

  The Department of Energy's Cybersecurity Risk Information Sharing Program (CRISP) leverages both classified and unclassified signatures to pinpoint activity unique to the Electricity and Oil and Natural Gas (ONG) entities. Any method or approach that encourages more natural gas industry participation would be beneficial to the entire Energy sector.

Testimony

Introduction and Background. Chairman Upton, Ranking Member Rush and members of the Subcommittee, thank you for the opportunity to testify. My name is Mark A. Engels and I'm a Senior Enterprise Security Advisor at Dominion Energy.

Dominion Energy is one of the nation's largest producers and transporters of energy, with a portfolio of approximately 26,200 megawatts of electric generation, 15,000 miles of natural gas transmission, gathering, storage and distribution pipelines and 6,600 miles of electric transmission and distribution lines. We operate the Cove Point liquefied natural gas (LNG) facility in Maryland, one of the largest natural gas storage systems in the U.S. with 1 trillion cubic feet of capacity, and serve more than 6 million utility and retail energy customers.

I have been with Dominion Energy almost 40 years with a focus on cybersecurity for 19 of those years. I'm an active member of the American Gas Association's (AGA) Cybersecurity Strategy Task Force and Natural Gas Security Committee; the Interstate Natural Gas Association of America's (INGAA) cyber and physical security committee; the Edison Electric Institute's (EEI) Security Committee; the Department of Homeland Security's (DHS) Classified Information Forum representing the Energy sector; a peer reviewer for the Department of Energy's (DOE) Cybersecurity for Energy Delivery Systems (CEDS) program; a member of the advisory team for Idaho National Laboratory's (INL) CyberCore Integration Center; and the former chair of the North American Electric Reliability Corporation's (NERC) Cyber Attack Task Force (CATF) and Attack Tree Task Force (ATTF).

On behalf of Dominion Energy, I appreciate the opportunity to provide comments and input to this Committee on HR 5174, the "Energy Emergency Leadership Act," and HR 5175, the "Pipeline and LNG Facility Cybersecurity Preparedness Act." I applaud the Committee's focus on advancing the public/private partnership between the Department of Energy and the Oil and Natural Gas sector. Neither will be successful without the other in addressing the continuous cyber and physical threats faced by our nation's pipelines .

Section 2(1) of HR 5175 directs the Department of Energy to establish policies and procedures to coordinate Federal agencies, States and the Energy sector.

Per the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD7), DOE is designated as the "Sector-Specific Agency" (SSA) for the Energy sector, which includes production, refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities. HSPD7 also designates DHS as the SSA for Transportation Systems sector, encompassing mass transit, aviation, maritime, ground/surface, and rail and pipeline systems. HSPD7 further states the Department of Transportation (DOT) and DHS will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines). As the SSAs, DOE and DHS are directed to be "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." In the case of natural gas pipelines and LNG, both DOE and DHS (in coordination with DOT) are the SSAs; DOE is the SSA for the natural gas commodity, and DHS (in coordination with DOT) is the SSA for the

pipeline infrastructure. The fact that natural gas pipelines have two SSAs, comprised of three Federal agencies (DOE, DHS, and DOT) cannot be understated, especially when it comes to interagency-coordination – in advance of, during, and post-incident operations. This coordination and acknowledgment of existing authorities – TSA regulatory authority for pipeline security (and associated incidents) and DOT regulatory authority for pipeline safety (and associated incidents) is critical to prevent duplication of efforts and to provide clarity to the owner/operator for effective security communication and outreach to the Federal government.

Additionally, the Homeland Security Act of 2002 directs DHS to be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. DHS is designated to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.

The key to this coordination is maintaining a productive relationship between the Energy Government Coordinating Council (EGCC), which is co-chaired by DOE's Office of Electricity Delivery and Energy Reliability (OE) and the DHS National Protection and Programs Directorate (NPPD), and the Oil and Natural Gas Sector Coordinating Council (ONGSCC). The ONGSCC is comprised of owners and operators from 20 plus industry trade associations representing all aspects of the ONG sector – drilling, exploration and production, processing, refining, services and supply, transmission, distribution and transportation (including pipelines) for liquid fuel and natural gas.

For many years, DOE's Office of Infrastructure Security and Emergency Response (ISER) has collaborated with the ONGSCC related to cyber and physical security to the mutual benefit of pipeline companies. The recent announcement of DOE's new Office of Cybersecurity, Energy Security and Emergency Response (CESER) should continue to improve the focus on pipeline cyber/physical security and coordination efforts.

A parallel relationship also exists between pipeline companies and the DHS's Transportation Security Administration (TSA). As the regulatory authority for pipeline security, TSA has demonstrated a long history of understanding pipelines and has the expertise to provide oversight to the industry.

In 2011, TSA released *Pipeline Security Guidelines*, which provide guidance on critical and non-critical pipeline asset security. The *Guidelines* were a collaborative effort of ONG asset owners, industry associations and TSA. These *Guidelines* have been the basis for cyber and physical protection implemented across the pipeline community. In 2016, TSA, again working with asset owners, industry associations, and the Department of Homeland Security's Industrial Control System's Cyber Emergency Response Team (DHS ICS-CERT), gathered input to update the *Guidelines* using the National Institute of Standards and Technology's (NIST) Cyber Security Framework as a model. The updated *Guidelines* are scheduled for release in the first half of 2018. Industry also provided input to augment the set of cybersecurity questions used in the Corporate Security Reviews (CSR) conducted by TSA.

Dominion Energy has a close working relationship with both ISER and TSA. In fact, TSA conducted a CSR of our pipeline cyber and physical security program in February, 2018. Also in attendance, at our invitation, were representatives from the General Accountability Office

(GAO), who is actively conducting their own assessment of TSA's cybersecurity capabilities. TSA identified eleven smart practices associated with our cyber and physical security program. But more importantly, they provided four recommendations that Dominion Energy will use to advance our security program. The CSR is an important part of the voluntary and collaborative partnership between TSA and industry. As a result of the partnership model, Dominion Energy has gained valuable insight from agencies with a wide view of the ONG sector.

Recommendation: While natural gas pipeline operators have a general idea about how the relevant Federal agencies associated with pipeline security should work together, HR 5175 would ideally encourage clarification on this issue. In HR 5174, Energy Emergency Leadership Act, the addition of paragraph 12 in the Department of Energy Organization Act, provides clarity and direction as well.

A more expedient approach may be to encourage a Memo of Understanding (MOU) between DOE and TSA that outlines roles and responsibilities for dealing with cyber and physical security for the ONG sector. This will immediately strengthen the relationship between these two key agencies. TSA already has an MOU with the DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) which has responsibility for pipeline safety. The TSA/DOT MOU has been critical to helping operators understand which Federal entity has the lead based on the type of incident (i.e., TSA is lead in the event of security-related incident, and PHMSA in the event of a pipeline safety incident).

Section 2(2) of HR 5175 directs the Department of Energy to coordinate response and recovery by Federal agencies, States and the Energy sector.

Dominion Energy conducts internal exercises to challenge our own staff and leaders. We recognize how important our services are to the health and safety of the public and to national security given the many critically important customers we serve. Our internal incident response plans outline how to engage with the different Federal and State agencies that we are likely to communicate with or from whom we request assistance. Dominion Energy procedures call for the ISER group to be the primary point of contact for our coordination with other Federal agencies such as the DHS, DOD and the FBI. Dominion Energy directly manages the coordination with our State partners through existing relationships.

DOE is very active in industry-led initiatives. For example, INGAA conducted a table-top exercise in April, 2017 involving a cyber and physical attack against a pipeline. Dominion Energy, along with 10 other INGAA members and staff from AGA, FERC, TSA, DOT and DOE participated. It was helpful for industry representatives to better understand the activities Federal agencies would perform during an event.

Dominion Energy also participated in NERC's bi-annual electric grid exercise (GridEX) which took place this past November. In addition, we invited our State Public Utility Commission staff and officials from the Virginia Governor's office to observe. While primarily targeting the electric grid, part of the scenario included malware attacks against natural gas pipelines and physical attacks on compressor stations serving electric generation. These injects allowed participants with natural gas assets to exercise their response plans as well as provide an opportunity for DOE to perform SSA duties for the entire Energy sector.

Dominion Energy plans to provide input to the Regional Integrated Energy Security Planning (RIESP) initiative, which was started in September 2017 by DOE, with assistance from INL and Argonne National Laboratory (ANL). By better understanding regional constructs, best practices, and data used by State governments to plan for response, DOE is looking to encourage greater regional energy security and resiliency planning by States.

Recommendation: The language in HR 5175 Section 2(2) blurs the presently clear distinction with States, actually adding complexity to a system that already has structure. Individual pipeline companies, Dominion Energy included, have longstanding relationships with State emergency response organizations, public utility commissions and law enforcement for all hazard events. Having DOE attempt to coordinate cyber and physical security for pipelines that could include all 50 States may not result in the value intended. This is particularly true for natural gas response and recovery, which is organized around time-tested local and regional coordination.

Section 2(3) of HR 5175 directs the Department of Energy to develop advanced cybersecurity applications and technologies.

In 2012, Dominion Energy was one of four utilities asked by DOE to collaborate on the development of the Cybersecurity Capability Maturity Model (C2M2). It was a great partnership example where industry guided, and DOE listened; exactly the way an effort like this should occur. The effort created a model that has been used by hundreds of electric and natural gas utilities. Dominion Energy has conducted C2M2 assessments against both our

electric and natural gas cybersecurity programs with results presented to our Board of Directors and used to drive improvements. DOE is now engaged in an effort to update the model, again leading by listening to industry for input.

Since 2012, I have been a peer reviewer for DOE's Cybersecurity for Energy Delivery Systems (CEDS) program. This effort has been incredibly important in advancing cybersecurity research and development efforts that have helped pipeline companies. CEDS resources are provided to leading vendors in the industry, academic institutions committed to advancing cybersecurity as well as DOE's national labs. By asking pipeline operators what works and what doesn't, when it comes to operational improvements, dollars are directed to initiatives that have the highest probability of being commercialized and integrated into the nation's natural gas pipeline infrastructure.

Following are two examples of CEDS initiatives that Dominion Energy has been involved with:

- One area that has proven to be a major vulnerability for industry involves Supply Chain threats. It is very difficult, if not impossible, for pipeline companies to have a level of assurance that the components and software integrated into operational infrastructure have the highest degree of integrity. INL has undertaken several initiatives to stand up test environments for Industrial Control Systems (ICS). One such initiative was called RENDER (Risk Evaluation Nexus for Digital Age Energy Reliability). RENDER created a three way sharing arrangement involving the lab, the vendor and the asset owner. Previous projects excluded the asset owner from the equation, creating uncertainty associated with remediation of the vulnerabilities identified by INL. With RENDER, the

asset owner not only could see what vulnerabilities were discovered, but provide input to the vendor about how critical or not the vulnerability was to the asset owner. This allowed the vendor to prioritize corrections that made the most sense to the asset owners.

RENDER targeted ICS used by both natural gas and electric utilities, but was only funded for an initial pilot. As a follow-up to RENDER, ISER is actively pursuing additional test-bed initiatives with multiple national labs that could assist both electric and natural gas utilities. It would not be a certification, but a more comprehensive test of key hardware and software with involvement of asset owners.

- Dominion Energy has taken advantage of DOE's Cybersecurity Procurement Language for Energy Delivery Systems. First published in 2014, the material has been used by our Supply Chain group to enhance the procurement process for our Gas Control Supervisory Control and Data Acquisition (SCADA) system.

Recommendation: HR 5175 should ensure adequate resources and funding to continue efforts like CEDS as well as test-beds for hardware and software testing. Through these programs vendors, academia, labs and industry gets involved and ultimately benefits arise from commercialization of products that meet industry requirements.

Section 2(4) of HR 5175 directs the Department of Energy to perform pilot demonstrations.

This section is complementary to Section 2(3) but goes further by directing actual demonstrations of technology.

Recommendation: Asset owners should be involved in the development of testing criteria to ensure the pilot represents, as close as possible, the real world environment the technology is intended to operate in.

Section 2(5) directs the Department of Energy to develop workforce development curricula.

One of the most effective and beneficial programs Dominion Energy staff participated in is *Cyber Strike*, a hands-on workshop, sponsored by DOE. *Cyber Strike* communicates the lessons learned from the 2015 and 2016 attacks on the Ukraine electric system. Dominion Energy staff from both our natural gas and electric SCADA teams attended workshops giving them practical experience in the type of offensive tactics and techniques they could face from an experienced adversary. Being able to learn from knowledgeable instructors is invaluable to our staff responsible for the safe and reliable operation of our control systems.

A CEDS funded INL initiative, Attack Technology and Characterization (*ATAC*), involved lab threat analysts training Dominion Energy SCADA engineering staff on a methodical approach to aggregate and evaluate cyber-risk related information.

Recommendation: HR 5175 should encourage more training and workforce development similar to *Cyber Strike* and *ATAC*, both of which have proven beneficial to Dominion Energy. To do this, DOE should involve asset owners to determine what programs work best.

Section 2(6) directs the Department of Energy to provide mechanisms to help the energy sector evaluate, prioritize and improve cyber and physical security capabilities.

Information sharing between the public and private sector is a foundational principle that helps the Oil and Natural Gas sector's efforts to address the continuously advancing threats that confront the sector. As will always be the case, there is never enough information, either classified or unclassified, and the information that is available can never be shared fast enough for industry.

The DOE OE has engaged the Energy Sector Information Sharing and Analysis Centers (ISACs), including the Oil and Natural Gas (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 (E-ISAC) to share and discuss cyber threat trends in a classified setting. Dominion Energy is a member of both the DNG-ISAC and the E-ISAC and benefits from intelligence provided by these organizations.

Dominion Energy has also participated in a pilot program, sponsored by DOE, to utilize Secure Video Teleconference (SVTC) capabilities. The purpose is to remotely convene a classified threat briefing for cleared industry representatives and reduce the amount of time it takes for actionable information to reach asset owners.

Along with approximately 30 electric utilities, Dominion Energy is part of DOE's Cybersecurity Risk Information Sharing Program (CRISP). Many of the participants have natural gas assets and automatically share information with the DOE and E-ISAC. This program leverages both classified and unclassified signatures to pinpoint activity unique to the Energy sector. The current CRISP program focuses on business networks, but efforts are also underway at INL to

provide a view into operational networks with a program called Cybersecurity for the Operational Technology Environment (CYOTE).

Recommendation: Any method or approach that encourages greater participation by ONG entities into the CRISP / CYOTE programs will have a positive impact on the entire Energy sector.

Conclusion: Dominion Energy and other natural gas pipeline companies have worked very closely with TSA and DOE on cyber and physical security to build a partnership based on trust and respect. This framework works because different organizations "stay in their swim lanes" and bring to the effort their specific area of expertise. DOE's coordination function is valuable in responding to a crisis and making available Federal resources to address the event. This support could come in the form of harnessing the considerable cybersecurity capabilities of the national labs, whose offensive and defensive threat analysts are world class, coordinating with DHS ICS-CERT for control system expertise or bringing to bear comprehensive knowledge of pipeline operations from TSA.

The proposed legislation should make sure that roles and responsibilities are clearly defined and understandable by pipeline operators who ultimately have to face the growing threat each and every day.

Thank you again for the opportunity to provide comments and input to this Subcommittee and I will be glad to answer any questions. Dominion Energy and I look forward to working with you on these important issues.