Congress of the United States

Washington, DC 20510

July 18, 2017

Dr. Huban A. Gowadia
Acting Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 22202

Dear Acting Administrator Gowadia:

We write today to request an assessment of current cyber and physical security protections for U.S. natural gas, oil, and other hazardous liquid pipelines and associated infrastructure. As you know, the Aviation & Transportation Security Act of 2001 created the Department of Homeland Security (DHS), and vested within the Transportation Security Administration (TSA) authority for pipeline security, including cybersecurity. Pursuant to the "Pipeline Security Guidelines" issued in April 2011, TSA relies on voluntary guidelines and guidance for the security of our nation's pipeline infrastructure.

An assessment of these guidelines and their effectiveness is needed as a number of major trends have emerged, with potentially significant implications for our energy, national and economic security. These include both the increasing interdependence of U.S. electric and natural gas infrastructure, and the evolving nature of cyber threats from both criminal and foreign state actors.

In 2005 Congress enacted legislation subjecting utilities and others to mandatory reliability, cybersecurity and physical security standards to protect the bulk power system. But we do not have a similar regime for natural gas pipelines even though natural gas accounts for approximately one-third of all U.S. electric generation. The reliability of the grid is now more than ever directly tied to the security of gas pipelines.

Like many grid systems, pipelines are now often operated through Supervisory Control and Data Acquisition (SCADA) systems, which allow greater operational efficiency—but are also more vulnerable to cyberattacks. Assessing the cybersecurity posture of our nation's pipeline infrastructure, associated federal policies and partnership efforts is timely and critical. The potential risks are grave, given that an attack on natural gas pipelines could, potentially, cripple the electric grid, which is a significant economic and national security asset.

We ask that the TSA pursue answers to the following questions:

1. Does the TSA take into account the interdependence of gas pipelines with the electric grid in assessing the "criticality" of the pipeline systems?

2. The Senate Committee on Energy and Natural Resources has heard testimony that many gas pipeline operators have undergone an assessment using the Department of Energy's Cybersecurity Capability Maturity Model. How many pipeline systems in the U.S. have undergone such an assessment? What percentage of industry does this represent? What kind of support is the federal government providing in these assessments?
3. For each year from FY 2010-FY 2016, how many gas pipeline operators have undergone a TSA inspection and review of their cybersecurity practices? What percentage of gas pipeline operators in the U.S have undergone such an assessment?
4. Does TSA's program of auditing and inspection follow a risk-based strategy based on criticality of pipeline infrastructure? If not, what is TSA's criteria for selecting the pipelines that have undergone inspections?
5. What is TSA's selection criteria for cybersecurity standards and metrics used in evaluating gas pipeline operators cybersecurity practices?
6. What percentages of pipeline operators are fully complying with every voluntary cyber security standard of TSA? If you do not have a definite percentage, what is your estimate?
7. To what extent, if at all, does the Federal Energy Regulatory Commission (FERC) review cybersecurity practices of gas pipeline operators? To what extent does FERC coordinate with TSA on cyber and physical security protections? What policies and procedures, memoranda of understanding, or any other documents govern coordination between FERC and TSA?
8. The Senate Committee on Energy Natural Resources has taken testimony on the Cyber Response Information Sharing Program, piloted by DOE and its national laboratories, designed to support the exchange of actionable threat information between government and industry through the Electricity Information Sharing and Analysis Center (E-ISAC), housed at the North American Electric Reliability Corporation. Does a similar program exist for the oil and gas pipeline sector?
9. How much real time data exchange occurs between the Electricity Information Sharing and Analysis Center, the Oil and Natural Gas Information Sharing and Analysis Center, and the Downstream Natural Gas Information Sharing and Analysis Center? How do these Information Sharing and Analysis Centers support cyber and physical security protections for the oil and gas pipeline sector, and are these efforts effective? Are there technology and structural barriers that prevent the most efficient information sharing? If so, what are they?
10. What are the research and development portfolio priorities of TSA and DHS with respect to pipeline cybersecurity? What is the annual federal expenditure on these activities, and to what extent do these programs leverage private sector investment? To what extent does coordination exist with the Department of Energy's Cybersecurity for Energy Delivery Systems?
11. How does DHS work with industry to identify critical infrastructure at greatest risk? How would a potential conflict under Executive Order 13636's sections 6 and 9 be resolved?

12. If Congress determines that mandatory cybersecurity standards are appropriate for the pipeline industry, which federal entity should enforce those standards?

The results of this assessment will help policymakers evaluate the security of our nation's energy assets, which are critical to the safety, security, and economic well-being of the country.

Thank you for your consideration.

Sincerely,

Maria Cantwell
Ranking Member, Senate Energy and Natural Resources Committee

Frank Pallone, Jr.
Ranking Member, House Energy and Commerce Committee