



U.S. Department of
Homeland Security

Written testimony of TSA Office of Security Policy and Industry Engagement Surface Division Director Sonya Proctor for a House Committee on Homeland Security, Subcommittee on Transportation Security hearing titled "Pipelines: Securing the Veins of the American Economy"

Release Date: April 19, 2016

311 Cannon House Office Building

Good afternoon Chairman Katko, Ranking Member Rice, and distinguished Members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in securing our Nation's pipeline systems.

The pipeline network is critical to the economy and security of the United States. More than 2.5 million miles of pipelines transport natural gas, refined petroleum products, and other commercial products throughout the country. In addition to the pipelines themselves, the system includes critical facilities such as compressor and pumping stations, metering and regulator stations, breakout tanks, and the automated systems used to monitor and control them. As evidenced by recent attacks in Brussels, Paris, and elsewhere, the terrorist threat has grown increasingly complex and diffuse, with the potential for terrorist actors to become radicalized and carry out an attack with little warning. An attack against a pipeline system could result in loss of life and have significant economic effects.

To ensure we remain vigilant, TSA works closely with the pipeline industry, which consists of approximately 3,000 private companies who own and operate the Nation's pipelines. Because they are usually unstaffed, securing pipeline facilities requires a collaborative approach across government and industry. TSA has established effective working relationships to ensure strong communication and sharing of intelligence, training resources, best practices, and security guidelines. Pipeline system owners and operators maintain direct responsibility for securing pipeline systems. TSA's role is to support owners and operators by identifying threats, developing security programs to address those threats, and encouraging and assisting the implementation of those security programs.

Stakeholder Engagement

TSA has established a productive public-private partnership with government partners and the pipeline industry to secure the transport of natural gas and hazardous liquids. On behalf of the Department of Homeland Security (DHS), TSA serves as a co-Sector Specific Agency alongside the Department of Transportation (DOT) and the United States Coast Guard (USCG) for the transportation sector. As part of the DHS-led Critical Infrastructure Partnership Advisory Council framework, TSA and DOT co-chair the Pipeline Government Coordinating Council to facilitate information sharing and coordinate on activities including security assessments, training, and exercises. TSA and DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) work together to integrate pipeline safety and security priorities, as measures installed by pipeline owners and operators often benefit both safety and security.

TSA engages pipeline industry stakeholders through the Pipeline Sector Coordinating Council (SCC), which provides a primary point of entry for industry representatives to discuss a range of pipeline security strategies, policies, activities, and issues with government. To eliminate the need for multiple meetings with the same security partners, TSA worked closely with the Department of Energy to ensure the Pipeline SCC also functions as the Pipeline Working Group within the Energy Oil and Natural Gas Sector.

Since the United States imports more petroleum from Canada than any other nation, much of it through pipelines, TSA works closely with our Canadian security counterparts to secure the U.S.-Canadian cross-border pipeline network. TSA and the Canadian National Energy Board coordinate closely on pipeline security matters to include exchanging information on assessment procedures, exercises, and security incidents. Since 2005, TSA and Natural Resources Canada have cosponsored the International Pipeline Security Forum, an annual two-day conference that enhances the security domain awareness of hazardous liquid and natural gas pipeline operators and provides opportunities for discussion of major domestic and international pipeline security issues. Administrator Neffenger had the pleasure of attending last year's Forum, and enjoyed the opportunity to engage with key industry leaders and learn more about their operations. The Forum presents a unique opportunity

for TSA to directly engage with a large number of pipeline industry leaders from the U.S. and Canada, as well as key government and law enforcement partners. Approximately 160 attendees participate in the annual Forum, including pipeline system owners and operators, pipeline trade associations, U.S. and Canadian government officials, and members of the security, intelligence and law enforcement communities from the U.S., Canada, and other countries.

Security Training and Guidelines

To assist pipeline owners and operators in securing their systems, TSA developed and distributed security training for industry employees and partners to increase domain awareness and ensure security expertise is widely shared. TSA's pipeline security training products include a security awareness training program highlighting signs of terrorism and each employee's role in reporting suspicious activity, an improvised explosive device awareness video for employees, and an introduction to pipeline security for law enforcement officers.

Additionally, TSA developed the TSA Pipeline Security Guidelines to provide a security structure for pipeline owners and operators to voluntarily use in developing their security plans and programs. The guidelines also serve as a standard for TSA's pipeline security assessments. TSA developed the guidelines with the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, pipeline trade associations, cybersecurity specialists, and other interested parties. Wide-spread implementation of this guidance by the pipeline industry has enhanced critical infrastructure security throughout the country. TSA is currently working with stakeholders to update these guidelines. The guidance has served as a template for entities establishing a corporate security program and has resulted in an increase in the quality of those programs reviewed by TSA. Since the publication of the guidelines, TSA has also seen an increase in the number of pipeline operators conducting security drills and exercises, an increase in coordination with local law enforcement agencies, and an increase in the number of operators conducting security vulnerability assessments of their critical facilities, all of which are recommended in the guidelines.

Exercises, Assessments, and Inspections

TSA works with industry partners to assess and mitigate vulnerabilities, and improve security through collaborative efforts including exercises, assessments, and inspections. With the support of Congress, TSA developed the Intermodal Security Training and Exercise Program (I-STEP). TSA facilitates I-STEP exercises across all surface modes, including pipelines, to help operators test their security plans, prevention and preparedness capabilities, threat response, and cooperation with first responders. TSA uses a risk-informed process to select the entities that receive I-STEP exercises and updates I-STEP

scenarios as new threats emerge to ensure industry partners are prepared to exercise the most appropriate countermeasures.

To identify shortfalls in pipeline security and develop programs and policies to enhance industry security practices, TSA conducts both corporate and physical security reviews with pipeline operators. While these reviews are voluntary, they have been welcomed by pipeline owners and operators who appreciate the value resulting from securing their systems.

Working with key executives and security personnel, TSA conducts the Corporate Security Review (CSR) program, which provides a company-wide assessment of operators' security policies, plans, and programs. Upon completion of each CSR, TSA provides recommendations to the company to enhance its physical and cyber security policies and plans. TSA has conducted over 140 CSRs since 2002, including six CSRs in Fiscal Year (FY) 2015 and four to date in FY 2016, with an additional four scheduled for completion by the end of the fiscal year. TSA has completed reviews of all 100 highest risk pipeline systems and is now conducting return visits to evaluate the implementation status of previous security recommendations.

TSA conducts field-based physical security reviews to assess security measures in place at pipeline critical facilities. The Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) required TSA to develop and implement a plan for inspecting the critical facilities of the top 100 pipeline systems in the nation. TSA conducted these required inspections between 2008 and 2011 through the Critical Facility Inspection program and is continuing the effort through TSA's Critical Facility Security Review (CFSR) program. Since 2008, TSA has conducted over 400 physical security reviews of critical facilities, with 46 CFSRs completed in FY 2015 and 21 completed to date in FY 2016, with 16 more expected to be completed by the end of this fiscal year.

Cybersecurity

In the pipeline mode, TSA supports DHS cybersecurity efforts in support of the National Institute of Standards and Technology Cybersecurity Framework. The cybersecurity framework is designed to provide a foundation that industry to better manage and reduce their cyber risk. TSA shares information and resources with its industry stakeholders to support their adoption of the framework. TSA also distributed a cybersecurity toolkit developed from DHS Critical Infrastructure Cyber Community C3 Voluntary Program materials and designed to offer the pipeline industry an array of no-cost resources, recommendations, and security practices. Additionally, within the pipeline industry, TSA is coordinating a voluntary cyber-assessment program with the Federal Energy Regulatory Commission to examine pipeline operators' cybersecurity programs. TSA works closely with

the pipeline industry to identify and reduce cybersecurity vulnerabilities, including facilitating classified briefings to increase industry's awareness of cyber threats.

Conclusion

Through voluntary programs and extensive engagement and collaboration, TSA works closely with government and industry stakeholders to secure the Nation's pipeline systems from terrorist attacks. TSA shares information with pipeline owners and operators, develops and distributes training materials and security guidelines, conducts security exercises, assessments, and inspections, resulting in an enhanced security posture throughout the pipeline industry. TSA continues to augment its efforts in the face of an evolving threat through the development and implementation of intelligence-driven, risk-based policies and programs. Thank you for the Subcommittee's support of TSA's goals and the opportunity to discuss these important issues.

Keywords: [Critical Infrastructure \(/keywords/critical-infrastructure/\)](/keywords/critical-infrastructure/), [Pipeline \(/keywords/pipeline/\)](/keywords/pipeline/).

Last Published Date: August 22, 2018