Statement of Sonya Proctor
Director, Surface Division
Policy, Plans, and Engagement
Transportation Security Administration
U.S. Department of Homeland Security
before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security
And
Subcommittee on Cybersecurity, Infrastructure Protection and Innovation
February 26, 2019

Good morning Chairmen Correa and Richmond, Ranking Members Lesko and Katko, and distinguished members of the Subcommittees. Thank you for the opportunity to appear before you to discuss the Transportation Security Administration's (TSA) efforts to secure surface transportation systems including oil and natural gas pipelines from cybersecurity risks.

TSA is committed to securing the transportation sector, which includes pipelines, against evolving and emerging risks, such as cyber-attacks. Partnering with our private sector partners to secure surface transportation from cyber-attacks is a critically important and complex undertaking. As the Director of National Intelligence recently stated, our adversaries and strategic competitors have cyber-attack capabilities they could use against U.S. critical infrastructure, including U.S. surface transportation. As a disruption to any of these systems would negatively impact our economy, commerce, and well-being, the cyber-attack threat is

driving the Department of Homeland Security's efforts to increase the cyber resilience of surface transportation.

Surface Transportation

The U.S. surface transportation system is a complex, interconnected, and largely open network comprised of mass transit systems, passenger and freight railroads, over-the-road bus operators, motor carrier operators, pipelines, and maritime facilities. The various modes that make up this system operate daily in close coordination with and proximity to one another. Americans and our economy depend on the surface transportation system operating securely and safely.

Every year more than 10 billion trips are taken on 6,800 U.S. mass transit systems, which range from small bus-only systems in rural areas to large multi-modal systems in urban areas. Over-the-road bus operators carry approximately 604 million intercity bus passengers each year. Over 3,300 commercial bus companies travel on the 4 million miles of roadway in the U.S. and on more than 600,000 highway bridges greater than 20 feet in length and through over 470 tunnels. Those same roads, bridges, and tunnels support the movement of goods throughout the country by eight million large capacity commercial trucks.

As for our railroads and pipelines, more than 570 individual freight railroads carrying essential goods operate on nearly 140,000 miles of track, and 2.75 million miles of pipelines, owned and operated by approximately 3,000 private companies, transport natural gas, refined petroleum products, and other commercial products.

TSA's functions and authorities as a security agency are uniquely structured to tackle the challenges at the intersections of surface transportation and cyber risks. To secure these

networks, TSA leverages its mature intelligence and analysis capability, along with its vetting and credentialing programs to ensure it can quickly develop and promulgate risk mitigation guidelines and measures to effectively coordinate and address evolving risk.

TSA's security efforts are bolstered by strong partnerships, trust, and collaboration with our federal and industry partners. In this regard, industry works with TSA to share their own unique vulnerabilities and security needs. Through this open communication, we collaboratively develop programs and guidelines for industry to voluntarily adopt to increase their overall security posture - an approach that has yielded significant security investments and improvements beyond what the agency would have achieved from a regulatory approach alone.

We believe that this voluntary and collaborative approach to developing and implementing security measures has been successful. However, we also recognize that should the need arise, based on an imminent threat or real-world event, the TSA Administrator has unique authority to require immediate implementation of certain security measures through the issuance of Security Directives (SDs).

TSA also actively collaborates with law enforcement entities, such as the Federal Bureau of Investigation (FBI), the Department of Justice, and the Joint Terrorism Task Force, to address attacks on critical infrastructure and supporting networks. For example, TSA works with the FBI to share intelligence information and host joint working groups on investigation and enforcement for attacks on surface transportation infrastructure. TSA also serves on the Energy Sector Government Coordinating Council, co-chaired by the Department of Energy and the DHS Cybersecurity and Infrastructure Security Agency (CISA), to discuss energy and pipeline security issues, provide insight on relevant intelligence, and coordinate at the federal level on pipeline-related security recommendations and programs. Additionally, TSA works closely with

the Pipeline and Hazardous Materials Safety Administration within the Department of Transportation for incident response and monitoring of pipeline systems.

TSA Cybersecurity Roadmap

In December of 2018, the TSA Administrator issued the agency's Cybersecurity Roadmap, which will guide efforts to prioritize cybersecurity measures within TSA and across the transportation system sector over the next five years. The Cybersecurity Roadmap identifies four priorities which will help the agency achieve its cybersecurity goals:

- Identify cyber security risks;
- Reduce vulnerabilities to our systems and critical infrastructure across the transportation systems sector;
- Mitigate consequences if and when incidents do occur; and,
- Strengthen security and ensure the resilience of the system.

The TSA Cybersecurity Roadmap has been supplemented with the development of an implementation plan which will assist in resource allocation to this critical area. In coordination with CISA, the Federal government's lead cybersecurity agency, the TSA Cybersecurity Roadmap brings TSA's cybersecurity efforts into alignment with both the National Cyber Strategy and the DHS Cybersecurity Strategy.

TSA's Cybersecurity Efforts for Surface Transportation

TSA approaches both cybersecurity and physical security by identifying, assessing, and mitigating any risks. TSA helps surface owners and operators identify vulnerabilities and risks in their operations, and works with them to develop and implement risk-mitigating solutions.

TSA's cybersecurity approach to its critical infrastructure mission is based on the National Institute of Standards and Technology (NIST) cybersecurity framework, which is designed to provide a foundation that industry can implement to sustain robust cybersecurity measures. TSA shares information and resources with industry to support adoption of the framework.

TSA cybersecurity resources and efforts for all modes of surface transportation include:

- *Cybersecurity Toolkit*: Provides information on an array of resources, recommendations, and practices available at no cost to surface transportation entities.
- *Cybersecurity Counterterrorism Guides*: "Pocket" resource guides to help educate all levels of surface transportation professionals on potential cyber threats, actions they can take, and best practices. Over 59,000 cybersecurity guides have been distributed across all modes of surface transportation.
- *Cybersecurity "5N5" Workshops*: Provides owners and operators of critical infrastructure with an awareness of existing cybersecurity support programs, resources, familiarity with the NIST Framework, and an opportunity to discuss cybersecurity challenges and share best practices. Workshop participants leave with immediate benefit by receiving five non-technical cybersecurity actions to implement over five days (5N5).
- *Cybersecurity Awareness Messages (CAMs)*: Disseminates information to stakeholders either in response to real-world events or in anticipation of significant anniversaries or holidays to support the transportation security

community's efforts to increase their cybersecurity posture, and recommends voluntary cybersecurity protective measures.

- *Daily Cybersecurity Reports*: The Public Transit and Over-the-Road Bus Information Sharing and Analysis Centers distribute daily cybersecurity awareness reports to their members.

Pipeline-specific cybersecurity efforts include:

- *TSA Pipeline Security Guidelines*: Initially developed in 2010 and revised in 2011, the Guidelines were revised again in 2018 to align with the NIST Cybersecurity Framework. TSA added a new cybersecurity section to more accurately reflect the current threat environment to help inform industry on how best to allocate their security resources based on their operations.
- *TSA-Federal Energy Regulatory Commission (FERC) Joint Voluntary Cyber Architecture Reviews*: Assesses the pipeline system's cyber security environment of operational and business critical network controls. These controls include the networked and segregated environments of Industrial Control System components, such as Supervisory Control and Data Acquisition, Distributed Control Systems, Remote Terminal Units, Human Machine Interfaces, and Process Logic Controllers.
- *Pipeline Cybersecurity Assessments*: DHS has established an initiative to evaluate the cybersecurity posture of critical oil and natural gas pipeline systems to determine their cybersecurity practices and promote resilience. TSA has partnered with CISA to develop on-site cyber assessments of key pipeline systems as part of the Pipeline Security Initiative. The assessments will provide pipeline owners

with a comprehensive evaluation and discovery process, focusing on defense strategies associated with asset owners' specific control systems network and segregated control assets. We plan to evaluate as many critical pipeline systems as possible on their cybersecurity posture by the end of this fiscal year (FY), as time and funding allows.

- *Corporate Security Review (CSR) Program and Critical Facility Security Review (CFSR) Programs*: CSRs are conducted to evaluate existing corporate security policies, procedures and practices, and make recommendations for improving existing corporate security posture. The TSA CSRs have been updated to include a more comprehensive and robust review of the cybersecurity policies, plans, and practices that the pipeline industry is employing. The CFSR program evaluates the top 100 most critical pipeline systems in the U.S., collecting site specific information from the facility operator on security policy, procedures and physical security measures. The CFSR program assessment questions have also been updated to include cyber specific measures.
- *Classified briefings*: TSA sponsors classified briefings for pipeline owners and operators. These briefings provide owners and operators with a need to know on updated pipeline cyber threat information.

Pipeline Security Success through Voluntary Actions

TSA had great success in working with the pipeline community to develop and implement voluntary guidance and programs to enhance their overall security programs and raise their baseline levels of security. Specifically, the pipeline community has been very supportive and receptive to our Pipeline Security Guidelines, including the addition of a comprehensive

cybersecurity section. The guidelines serve as the de facto standard for pipeline security programs, and were developed in close coordination with the pipeline industry. Major pipeline industry associations continue to show support of and collaboration with the measures set forth in the guidelines. Associations such as the American Gas Association, the Interstate Natural Gas Association of America, and the American Petroleum Institute, have written "membership statements" committing to voluntary adherence to the Pipeline Security Guidelines.

Pipeline operators have shown a willingness and ability to voluntarily implement the mitigation measures set forth in the guidelines. We have strong evidence that an industry-backed voluntary program to reduce risk by increasing compliance with the guidelines is working. TSA conducted 23 CSRs in FY 2018, and those pipeline operators assessed had a 90% compliance rate regarding Corporate Security Program Management; an 85% compliance rate regarding Security Incident Management; and an 80% compliance rate regarding the TSA recommended cybersecurity practices detailed in the 2011 Guidelines. In addition, we have seen a strong increase in corporate compliance when comparing results from a second review to a company's first review. For 10 companies where we have conducted a second CSR, we have seen the number of recommendations made decrease from a total of 446 recommendations (first review) to 146 (second review). In addition, companies have implemented corrective actions on over 81% of the recommendations made during our CFSRs. This very high rate regarding corrective actions is indicative of industry acceptance and adherence to TSA Guidelines. In FY 2019, we will compile similar CSR data based on the updated 2018 Guidelines, which will help determine how and where we apply additional resources to the pipeline industry.

Conclusion

In closing, TSA has been able to support the improvement of both physical and cyber security across all surface modes of transportation, including pipelines, thanks to the trust and relationships we have cultivated with our federal partners and industry. As evidenced by the programs and resources TSA has collaboratively developed and implemented for our surface transportation stakeholders, TSA is committed to securing the Nation's surface transportation system from terrorist and cybersecurity attacks. TSA looks forward to working with Congress on these efforts. Thank you for the opportunity to discuss these important issues. I look forward to the Subcommittees' questions.