Written Testimony of

Sonya T. Proctor

Assistant Administrator, Surface Operations

Security Operations

Transportation Security Administration

U.S. Department of Homeland Security

Hearing on

"Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack"

Before the

Committee on Homeland Security

Subcommittee on Transportation and Maritime Security

and

Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.

June 15, 2021

Good morning, Chairwomen Watson Coleman and Clarke, Ranking Members Gimenez and Garbarino, and distinguished Members of the Subcommittees. 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.

TSA has engaged with the pipeline industry since 2001 and has taken clear and specific actions to address cybersecurity gaps and vulnerabilities with the pipeline industry. Our Nation's pipeline systems are vital to the economy, our National Security, and the livelihood of our country. There are more than 2.8 million miles of natural gas and hazardous liquid pipelines owned and operated by over 3,000 private companies. Besides the pipelines themselves, the system includes critical facilities such as compressor and pumping stations, metering and regulator stations, interconnects, main line valves, tank farms and terminals, and the automated systems used to monitor and control them. Pipelines are susceptible to physical attacks such as improvised explosive devices (IEDs) and vehicle borne IEDs, small arms, and stand-off weapons. Additionally, as recently evidenced, cyber intrusions into pipeline computer networks have the potential to negatively impact our national security, economy, commerce, and well-being. For these reasons, TSA remains committed to securing our Nation's pipelines against evolving and emerging risks.

Pipeline Staffing, Resourcing, and Expanding Internal Capabilities

TSA has historically devoted staff to developing surface transportation policies supporting the grant process for surface transportation-related security enhancements, and conducting inspections and assessments. In support of the TSA Modernization Act of 2018 (H.R. 302), in October 2019, TSA established the office of Surface Operations under the Office

of Security Operations, which reports to the Executive Assistant Administrator for Security Operations. During this time TSA expanded its pipeline security staff from six positions to 34 positions working in field operations, headquarters operations, and policy development. These resources allow TSA to advance our pipeline and cybersecurity mission.

In Fiscal Year (FY) 2020, TSA created and trained a field-based 20-member Pipeline Security Assessment Team (PSAT), which is comprised of Transportation Security Inspectors (TSIs) located around the Nation. For cybersecurity efforts, we now have eight members from the PSAT team and headquarters who successfully completed comprehensive cybersecurity training, provided by Idaho National Labs (INL) in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), and are receiving additional cybersecurity certification in support of TSA's pipeline cybersecurity mission.

TSA continues to expand its cybersecurity staffing and resourcing capabilities through establishing a Cybersecurity Operations Support Branch, which is currently in the hiring process. The branch will be staffed by 11 specialized cybersecurity personnel, six of which will be hired in FY2021 as part of 34 positions as previously mentioned. Five additional cyber security personnel will be hired in FY2022. This new branch within Surface Operations aims to enhance transportation systems' cybersecurity posture through a multi-layered approach, which includes conducting cybersecurity assessments and engagements; targeted stakeholder educational efforts; evaluation of cybersecurity best practices across the sector; and government coordination and collaboration on surface cyber programs and engagements.

The TSA Surface Policy Division within the Office of Policy, Plans, and Engagement is also increasing its cybersecurity efforts and will have a total of nine positions by the end of

FY2021 to expand its Cybersecurity Section. This section will focus on the development of cybersecurity-related policy and guidance for surface transportation security.

Stakeholder Partnership

TSA's focus on pipeline security began in 2001 and through our expanding pipeline efforts, we have focused on enhancing the security preparedness of the Nation's hazardous liquid and natural gas pipeline systems. TSA has established a productive public-private partnership with government partners and the pipeline industry to protect the transport of hazardous liquids and natural gas. This partnership includes collaboration with our federal partners, such as Department of Homeland Security (DHS), the Department of Transportation (DOT), the Department of Energy (DOE), the Department of Justice (DOJ), and the Federal Energy Regulatory Commission (FERC) through the Energy Government Coordinating Council (EGCC), while providing input and support to the activities and initiatives of the industry-led Oil and Natural Gas Subsector Coordinating Council (ONG SCC) and the Pipeline Working Group (PWG). Through these partnerships, TSA continues to seek input on current efforts to develop mandatory cybersecurity measures in Security Directives (SD); collaboratively develops security guidelines and training materials, and offer cybersecurity assessments for pipeline industry partners to increase security awareness and preparedness.

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

security for law enforcement officers; a cybersecurity toolkit for small and midsize businesses offering guidance on how to incorporate cyber risk into their transportation system; and a pocket-sized guide for frontline employees to outline the most common types of cybersecurity threats and explain how transportation systems can protect their data, computer systems, and personal information.

Additionally, in conjunction with the pipeline industry, TSA developed the TSA Pipeline Security Guidelines (Guidelines) in 2011 to provide a security structure for pipeline owners and operators to use in developing their security plans and programs. The Guidelines are non-regulatory but recommended security measures for both physical and cyber security that serve as the de facto industry standard. The Guidelines were updated and republished in March 2018 with a significant emphasis on cybersecurity measures that are aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework. In April of this year, the criteria for identifying critical pipeline facilities in the Guidelines were further updated. The Guideline's cybersecurity measures were developed in coordination with industry and with Industrial Control System (ICS) expertise from the Cybersecurity and Infrastructure Security Agency (CISA).

Established by TSA in 2019, the Surface Transportation Security Advisory Committee (STSAC) consists of 35 industry voting members, of which three are pipeline subject matter experts, and 14 government non-voting members. This committee advises, consults with, reports to, and makes recommendations to the TSA Administrator on surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

Exercises, Assessments, and Site Reviews

TSA works with industry partners to assess and mitigate vulnerabilities, and improve security through collaborative efforts including intelligence briefings, exercises, assessments, and on-site reviews. Through the Intermodal Security Training and Exercise Program, TSA provides exercises, trainings, and security planning tools to the pipeline community to strengthen company security plans, policies, and procedures. Working with pipeline operators' security personnel, TSA conducts Pipeline Corporate Security Reviews, which assess the degree to which the Pipeline Security Guidelines' physical and cyber security measures are integrated into the operator's corporate security plan.

In addition, TSA also conducts Pipeline Critical Facility Security Reviews on critical pipeline facilities of the 100 most critical pipeline operators to collect site-specific information on facility security policies, procedures, and cyber and physical security measures. To promote a secure and resilient cybersecurity posture, through specific Congressional funding TSA works directly with CISA to collaborate with pipeline owners and operators to offer Validated Architecture Design Reviews to assess a pipeline operator's critical infrastructure including information technology (IT) and operational technology (OT) systems. This assessment is intended to determine if OT systems are designed, built, and operated in a reliable and resilient manner. This assessment examines a series of cybersecurity technical domains that goes beyond a questionnaire-type assessment and also includes traffic analysis from selected critical network segments as well as a network architecture diagram and functionality review. While these security reviews are not mandatory, they have been welcomed over the years by pipeline owners and operators who appreciate and understand the value of identifying and mitigating vulnerabilities to help better secure their physical and cyber systems.

Cybersecurity

On behalf of the Department of Homeland Security, TSA serves as the co-Sector Risk Management Agency alongside DOT and the United States Coast Guard for the transportation systems sector and is responsible for developing, deploying, and promoting Transportation Systems Sector-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information sharing products that support the implementation of Executive Orders on cybersecurity. TSA is in close alignment with CISA and coordinates on both a tactical and strategic level to raise the cybersecurity baseline across the transportation sector. As noted earlier, TSA participates in the Energy Government Coordinating Council and regularly collaborates with the ONG SCC and its PWG on programattic issues affecting the cybersecurity of pipeline systems.

TSA supports DHS's cybersecurity efforts in alignment with the NIST Cybersecurity Framework (Framework). The Framework is designed to provide a foundation for industry to better manage and reduce their cyber risk. TSA shares information, resources, and develops products for stakeholders to support their adoption of the Framework. 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.

In response to the recent pipeline cyber intrusion, TSA is using its statutory authority to strengthen the cybersecurity and resilience of pipeline owners and operators. The first security directive issued following the recent incident requires pipeline owners and operators of critical hazardous liquid and natural gas pipelines or a liquefied natural gas pipelines facility designate a Cybersecurity Coordinator; report cybersecurity incidents to CISA; and assess their current

cybersecurity posture against a specific set of measures within the Pipeline Security Guidance. As part of this assessment, the owner/operators must identify any gaps, develop a remediation plan if necessary, and report the results to TSA.

All information reported to CISA pursuant to this directive is shared with TSA and other federal agencies as appropriate. Similarly, all information provided to TSA is shared with CISA. By requiring the reporting of cybersecurity incidents, the federal government is better positioned to understand the changing threat of cyber events and the current and evolving risks to pipelines. The designation of Cybersecurity Coordinators will give TSA a known and consistent point of contact with critical pipeline owners and operators, allowing TSA to easily share security information and intelligence. The assessments will assist the owners and operators and TSA to better understand the current state of cybersecurity practices in individual companies and across the industry. In addition, TSA, in close coordination with the Department and CISA, is also exploring ways in which immediate threats, such as ransomware, can be mitigated through additional cybersecurity measures to ensure that critical pipeline owners and operators are engaging in baseline cyber hygiene and have contingency plans in place to reduce the risk of significant disruption of operations, if a breach occurs.

Conclusion

The pipeline system is crucial to U.S. national security, transportation, and energy supply. These pipelines provide connections to other critical infrastructure upon which we depend, such as airports and power plants. TSA is dedicated to protecting our Nation's pipeline networks against evolving threats and continues to work collaboratively with our government and private partners to expand the implementation of intelligence-driven, risk-based policies, and

programs. TSA is committed to using its authority to implement the appropriate security measures to elevate both the physical and cyber security posture of the pipeline industry in alignment with the threat environment. Thank you for the opportunity to discuss TSA's Pipeline Security Program and I look forward to your questions.