Written Testimony of David P. Pekoske

Administrator

Transportation Security Administration

U.S. Department of Homeland Security

Hearing Pipeline Security

Before the

Committee on Commerce, Science, and Transportation

July 27, 2021

Good morning, Chair Cantwell, Ranking Member Wicker, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in pipeline security.

The nation's pipeline systems illustrate how vital critical pipeline systems are to the economy, our national security, and the livelihood of our country. Safeguarding these systems is a critical undertaking and requires extensive collaboration with pipeline owners and operators. The United States has more than 2.8 million miles of natural gas and hazardous liquid pipelines owned and operated by over 3,000 private companies. In addition to the pipelines themselves, the systems include critical facilities such as compressor and pumping stations, metering and regulator stations, interconnects, main line valves, tank farms and terminals, and automated systems used to monitor and control these facilities. Pipelines are susceptible to physical attacks and other acts of tampering and sabotage. Cyber intrusions into pipeline computer networks have the potential to negatively impact our national security, economy, commerce, and well-being.

Pipeline Staffing, Resourcing, and Expanding Internal Capabilities

To support the surface transportation security mission, TSA has developed surface transportation policies and regulations; supports the grant process for surface transportation-related security enhancements; conducts inspections and assessments of surface transportation operators to identify risk and provide risk mitigation strategies; and provides workforce training and exercise support. In response to the *TSA Modernization Act*, in October 2019, TSA established the Surface Operations office, which reports to the Executive Assistant Administrator for Security Operations. This organization is led by an Assistant Administrator and Deputy Assistant Administrator, both members of the Senior Executive Service, at TSA Headquarters, and five Regional Security Directors in the field, all at the Senior Executive Service level. The Regional Security Directors and their supporting staff have direct operational oversight of approximately 200 Surface Transportation Security Inspectors deployed in 47 field offices across the country. Since the passage of the *TSA Modernization Act*, TSA has expanded our pipeline security staff from six to 39 Full Time Equivalents (FTEs) working in field operations, headquarters operations, and policy development. These resources, both in our headquarters and in the field have allowed us to substantially increase our surface transportation security capability.

Further, in Fiscal Year (FY) 2020, TSA established and trained a 20-member field-based Pipeline Security Assessment Team (PSAT), which is comprised of credentialed Transportation Security Inspectors (TSIs) located around the nation in order to expand TSA's support and engagement capacity with pipeline owners and operators. For cybersecurity efforts, we now have eight members from the PSAT team and TSA headquarters who completed comprehensive cybersecurity training, provided by Idaho National Labs. This was done in partnership with the

Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and we are receiving additional cybersecurity certification in support of TSA's pipeline security mission.

TSA continues to expand its cybersecurity staffing and resourcing capabilities through the establishment of a Cybersecurity Operations Support Branch embedded within Surface Operations. As part of the 39 FTE previously mentioned, staffing for this Cyber Branch will include an additional 10 specialized cybersecurity personnel, all of whom are expected to be onboard in the next 60 days. This increase is a direct result of the Cyber Workforce Initiative implemented by DHS this year that allows direct hiring for individuals with the appropriate cybersecurity expertise. In addition to these newly hired cybersecurity experts, TSA has positioned additional field-based TSIs to undergo cybersecurity training and are on a career path to become cyber assessors within the surface transportation environment. This newly established field-based team will create an additional capability for local level cybersecurity outreach and establish a model for future professional cybersecurity career progression within TSA.

We will continue to evaluate and support implementation of cybersecurity best practices across the transportation sector and collaborate with other government agencies on surface cyber programs and engagements.

The TSA Surface Policy Division within the Policy, Plans, and Engagement office, in Operations Support, is also increasing its cybersecurity efforts and will expand its workforce specializing in cybersecurity from six positions to a total of nine within the next 60 days. This resource will focus on the development of cybersecurity-related policy and guidance for surface transportation security.

Stakeholder Partnership

In 2003, TSA began assessing the state of security in the pipeline industry through its Corporate Security Review (CSR) program. The goals of the program were to develop first-hand knowledge of the security measures in place at critical pipeline sites and establish working relationships with key pipeline security personnel including the industry-established Oil and Natural Gas Sector Coordinating Council (ONG SCC). The initial CSRs identified smart security practices and laid the groundwork for TSA's Pipeline Security Guidelines. The Pipeline Security Guidelines, required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, went into effect in 2011 and with a 2018 revision, are still in use today and updated as necessary.

These Pipeline Security Guidelines provide a security structure for pipeline owners and operators to use in developing their security plans and programs and contain recommended security measures for both physical and cyber security that serve as the de facto industry standard. The Pipeline Security 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. The guideline's cybersecurity measures were developed in coordination with industry and with Industrial Control System (ICS) expertise from CISA. In April of this year, the criteria for identifying critical pipeline facilities in the guidelines were further updated.

Through our efforts to expand pipeline security, we have focused on enhancing the security preparedness of the nation's hazardous liquid and natural gas pipeline system. TSA has established a range of productive public-private partnerships to protect the transport of hazardous liquids and natural gas. This partnership includes collaboration with our federal partners, such as

CISA, the Department of Transportation (DOT), the Department of Energy, and the Department of Justice. We are also partnering with the Federal Energy Regulatory Commission through the Energy Government Coordinating Council (EGCC). In addition, TSA is providing input and support to the activities and initiatives of the ONG SCC and the Pipeline Working Group (PWG), which also serves as the Pipeline Subsector Coordinating Council (PSCC) of the Transportation Systems Sector.

To support pipeline owners and operators in securing their systems, TSA develops and regularly distributes security training materials for industry employees and partners to increase domain awareness and ensure security expertise is widely shared. These 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, and an introduction to pipeline security for law enforcement officers. To address cyber threats, the training materials, available since 2017, contain a cybersecurity toolkit for small and midsize businesses, offering guidance on how to incorporate cyber risk into their transportation system. Also included is a pocket-sized guide for frontline employees that outlines the most common types of cybersecurity threats and explains how transportation systems can protect their data, computer systems, and personal information.

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 (I-STEP), TSA provides the pipeline community with exercises, training, and security planning tools to

strengthen company security plans, policies, and procedures. To date, TSA has conducted 21 I-STEP tabletop exercises specific to pipelines, with pipeline companies participating in numerous other exercises more broadly focused on all modes of transportation. Working with pipeline operators' security personnel, TSA conducts Pipeline CSRs, which assess the degree to which the Pipeline Security Guidelines' physical and cybersecurity measures are integrated into the operator's corporate security plan.

TSA also conducts Critical Facility Security Reviews on critical pipeline facilities for the most critical pipeline owners and operators to collect site-specific information on facility security policies, procedures, and physical security measures.

TSA is a partner with CISA's National Risk Management Center in the Pipeline Cybersecurity Initiative (PCI). The initiative was launched in 2018 to assist pipeline owners and operators to prepare for and respond to significant cyber events. Through the PCI initiative CISA, TSA, and Idaho National Laboratory assess the cybersecurity posture and preparedness of pipeline companies, analyze assessment findings to develop risk mitigation strategies and identify support and informational tools that companies may use to address identified risks.

To promote a secure and resilient cybersecurity posture, TSA works directly with CISA to collaborate with pipeline owners and operators to offer cybersecurity 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, secure, and resilient manner. This assessment goes beyond a questionnaire-type assessment and includes traffic analysis from selected critical network segments. Pipeline owners and operators have expressed appreciation

for these reviews over the years, understanding the value of identifying vulnerabilities to help better secure their physical and cyber systems.

Cybersecurity

On behalf of DHS, the Co-Sector Risk Management Agency for the Transportation Systems Sector (TSS) along with DOT, TSA serves as the executive agent with the U.S. Coast Guard for TSS and is responsible for developing, deploying, and promoting TSS-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information-sharing products. 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 EGCC and regularly collaborates with the ONG SCC and the PWG/PSCC on programmatic issues affecting the cybersecurity of pipeline systems.

TSA also 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 and 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.

Colonial Pipeline Incident

On May 7, 2021, the Colonial Pipeline Company announced it halted its pipeline operations due to a ransomware attack. This incident temporarily disrupted critical supplies of gasoline and other refined petroleum products throughout the East Coast. This was not the first

cyber intrusion in our nation to have a direct impact and cybersecurity incidents affecting surface transportation systems continue to be a growing and evolving threat.

In response to this cyber intrusion, TSA exercised its *Aviation and Transportation Security Act of 2001* authorities to strengthen the cybersecurity and resilience of pipeline owners and operators by issuing two Security Directives. The first Security Directive issued by TSA following the Colonial Pipeline incident requires pipeline owners and operators of critical hazardous liquid and natural gas pipelines or a liquefied natural gas pipeline facility to designate a Cybersecurity Coordinator who is required to be available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise. The Cybersecurity Coordinator is also required to report significant cybersecurity incidents to CISA and assess their current cybersecurity posture against a specific set of measures within the Pipeline Security Guidelines. As part of this assessment, the owners and operators must identify any gaps, develop a remediation plan if necessary, and report the results to TSA and CISA.

All information reported to CISA pursuant to the Security Directive is securely shared with TSA and other federal agencies as appropriate. Similarly, all information provided to TSA is securely shared with CISA and other federal agencies as appropriate. By requiring the reporting of significant cybersecurity incidents, the federal government is better positioned to understand the constantly 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 rapidly share security information and intelligence. The assessments will assist owners and operators and TSA to better understand the current state of cybersecurity practices in individual companies and across the industry.

TSA is pleased to report that all of the designated owner/operators have complied with requirements in the first Security Directive, including conducting a self-assessment within 30 days, naming a Cybersecurity Coordinator, and informing TSA of the designated individual and alternate(s). This is a testament to the long-standing security partnership developed over the years between TSA and this critical sector and industry's commitment to fulfill their required security responsibilities and take action on this evolving threat. TSA, in partnership with CISA, is in the process of analyzing all assessments to identify further mitigation efforts.

In response to the ongoing cybersecurity threat to pipeline systems, on July 19, 2021, TSA issued a second Security Directive that requires owners and operators of TSA-designated critical pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections against cyber intrusions.

The second Security Directive was developed in close coordination with federal partners, including subject matter experts from CISA. TSA consulted with industry on the Security Directive and took their comments into consideration, including updating the security directive to incorporate some of the feedback received. The second Security Directive requires owners and operators of TSA-designated critical pipelines to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review.

Conclusion

The pipeline system is crucial to U.S. national security, transportation, and our energy supply. These pipelines provide connections to other critical infrastructure upon which we

depend, such as power plants and the aviation gasoline fuel supply for airplanes. 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 ensuring appropriate security measures are in place to increase the physical and cyber security posture of the natural gas and hazardous pipeline industry sub-sector in alignment with the risks this system faces. Thank you for the opportunity to discuss TSA's efforts to strengthen pipeline security, and I look forward to your questions.