Written Testimony of Victoria Newhouse
Deputy Assistant Administrator Transportation Security Administration
U.S. Department of Homeland Security

Hearing Before the
House Transportation and Infrastructure Committee
"The Evolving Cybersecurity Landscape:
Federal Perspectives on Securing the Nation's Infrastructure"
December 2, 2021

Good morning, Chairman DeFazio, Ranking Member Graves, and distinguished Members of the Committee. My name is Victoria Newhouse and I serve as the Deputy Assistant Administrator for Policy, Plans, and Engagement within the Transportation Security Administration (TSA). I appreciate the opportunity to appear before you today to discuss TSA's role in cybersecurity for our Nation's infrastructure.

TSA was established by the *Aviation and Transportation Security Act* (ATSA), which was signed into law on November 19, 2001. With the enactment of ATSA, TSA assumed the mission to oversee security in all modes of transportation, be that aviation or the Nation's surface transportation systems – mass transit and passenger rail, freight rail, highway and motor carrier, pipeline, as well as supporting maritime security with our U.S. Coast Guard (USCG) partners. As we recently observed TSA's 20th anniversary, we rededicated ourselves to our critical mission to protect our Nation's transportation systems as they remain attractive targets for our adversaries to directly attack our Homeland, our commercial markets, and ultimately the freedoms we hold so dear. My personal commitment to TSA's important mission to ferociously protect our Homeland is fueled by my own experience on September 11, 2001, surviving the attack on the Pentagon on that fateful day when we lost 2,977 friends, family members and colleagues. This is not a mission we can accomplish alone. TSA's mission success is highly dependent on close

collaboration and strong relationships with our transportation industry stakeholders and our Federal agency partners, including several who are present on this esteemed panel today. TSA's motto -"not on my watch" – truly reflects our collective approach to secure our Homeland against all threats, including cybersecurity threats.

Transportation Cybersecurity Threats

Cybersecurity incidents affecting transportation are a growing, evolving, and persistent threat. Across U.S. critical infrastructure, cyber threat actors have demonstrated their willingness and ability to conduct malicious cyber activity targeting critical infrastructure by exploiting the vulnerability of Internet-accessible Operational Technology (OT) assets and Information Technology (IT) systems. Malicious cyber actors continue to target U.S. critical infrastructure, to include transportation systems, through malicious cyber activity and cyber espionage campaigns. For instance, the ransomware incident against Colonial Pipeline last May underscores this threat. The United States' adversaries and strategic competitors will continue to use cyber espionage and malicious cyber activity to seek economic, political and military advantage over the United States and its allies and partners. TSA is dedicated to protecting our Nation's transportation networks against evolving threats and continues to work collaboratively with public and private stakeholders to expand the implementation of intelligence-driven, risk-based policies and programs and continue robust information sharing to reinforce the security posture of these networks.

Addressing Cybersecurity Threats

As reflected in cybersecurity and infrastructure testimony provided by industry colleagues to this committee on November 4, 2021, the United States has a vital national interest in understanding, mitigating, and protecting its people and infrastructure from cybersecurity threats in the transportation domain. The constantly evolving potential for malicious cyber activity against the transportation infrastructure point to the need for continued vigilance, information sharing, and development of dynamic policies and capabilities to strengthen our cybersecurity posture. Consistent with the President's *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 28, 2021), Department of Homeland Security priorities, and our broader statutory authorities, TSA has sought to mitigate

the "degradation, destruction, or malfunction of systems that control this infrastructure" by implementing immediate security requirements through security policies.

After the Colonial Pipeline ransomware incident in May, there was a clear understanding across the Administration, Congress, industry, and the public for the need to take action to prevent another pipeline incident in the future. The TSA Administrator leveraged authority under 49 U.S.C. §114 to respond to emerging threats by directing select owners and operators of pipeline and natural gas facilities to implement necessary cyber protections. TSA issued two Security Directives (SDs), effective May 28, 2021, and July 26, 2021, to immediately address these threats. Among several requirements, the SDs required pipeline companies to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA), designate a cybersecurity coordinator to be available 24/7, and implement specific mitigation measures to protect against ransomware incidents.

Credible cyber threat information also supported our recent efforts to implement similar security measures across the domestic surface and aviation transportation networks. In the surface domain, new cybersecurity protocols require higher risk freight railroads, passenger rail and rail transit operators to take four critical actions:

1. Designate a cybersecurity coordinator;
2. Report cybersecurity incidents to CISA;
3. Develop a cybersecurity incident response plan to reduce the risk of an operational disruption; and
4. Conduct a cybersecurity self-assessment to identify potential gaps or vulnerabilities in their systems.

In addition to these requirements, TSA also issued an Information Circular to lower risk surface transportation operators, including over-the-road buses and lower risk rail operators, strongly recommending they immediately implement these same measures.

Within the aviation subsector, TSA recently updated established security programs with these same measures, starting with designating a cybersecurity coordinator and reporting specific cybersecurity incidents to CISA. In a second set of security program updates to be issued in the

near future, TSA will also implement the requirements to conduct cybersecurity self-assessments and develop cybersecurity incident response plans.

DHS and TSA engaged with stakeholders throughout the development process for these measures to ensure awareness of the threat picture, review draft proposals, and obtain industry feedback. This included stakeholder CEO-level discussions with DHS and TSA leaders, threat briefings for aviation, pipeline, and other surface transportation stakeholders, multiple policy reviews by industry and government stakeholders, and consistent engagement sessions with transportation associations and regulated entities for awareness on the proposed strategies. For example, we engaged TSA's Surface Transportation Security Advisory Committee (STSAC) on several occasions to share and discuss these new security requirements and held numerous stakeholder calls and engagements with the specific covered operators prior to issuing these most recent security requirements. In addition, airport and airline stakeholders also provided extensive input to our aviation cyber requirements to ensure they can operationalize them effectively and efficiently. Our interagency partners also participated extensively to ensure unity of effort across DHS and the interagency. We incorporated stakeholder inputs resulting in revisions to these cybersecurity policy requirements, including adjustments to incident reporting and response plan timeframes, defining reportable cybersecurity incidents, and using established methods to conduct self-assessments. We continue working closely with stakeholders to assist with implementation and respond to any questions regarding these requirements with an eye on continually improving our collective efforts to secure the Nation's transportation systems from cyber threats.

Information Sharing and Engagement

Our work does not simply end after issuing these cybersecurity requirements. On the contrary, the TSA enterprise continues our robust stakeholder engagement to mitigate cyber threats. We work closely with these covered operators to successfully implement these requirements, educate our vast network of transportation operators, and continue to seek input from both the STSAC and the Aviation Security Advisory Committee (ASAC) on how to best integrate cybersecurity into the fabric of our transportation security mission. For example, we have sought, incorporated, and continue to seek stakeholder input, including from those advisory

committees, on TSA's Cybersecurity Roadmap. TSA conducts robust outreach with thousands of individual transportation operators to implement these requirements and ensure consistent application across the transportation sector. We continually seek opportunities to expand information exchanges and to provide evaluation tools and training programs to evaluate systems, identify vulnerabilities, and incorporate security measures and best practices that mitigate cyber threats. This includes efforts such as the Baseline Assessment for Security Enhancement (BASE) program and the Intermodal Security Training and Exercise Program (I-STEP). TSA actively supports broader DHS efforts, such as the 60-day Transportation Cybersecurity Sprint in September and October that focused on enhancing cyber risk management and cybersecurity in the context of the transportation sector with particular emphasis on TSA, CISA, and USCG engagements.

On behalf of DHS, TSA and USCG are the Co-Sector Risk Management Agency for the Transportation Security Sector (TSS) along with the Department of Transportation (DOT). In that role, TSA serves as the executive agent with the USCG 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.

TSA also supports DHS's cybersecurity efforts in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Framework). The Framework is designed to provide a foundation for industry to better manage and mitigate their cyber risk. TSA shares information and resources and develops products for stakeholders to support their adoption of the Framework. For example, TSA in conjunction with the USCG and the DOT, has been working with NIST to develop transportation-specific profiles for the Framework through a series of sector surveys to allow for further targeted sector adoption of the Framework.

Robust information and intelligence sharing is a key enabler of TSA's mission to protect the nation's transportation systems to ensure the freedom of movement for people and commerce. TSA coordinates with the DHS Office of Intelligence and Analysis and Intelligence Community

(IC) partners across the federal government to share cyber threat information with industry as soon as it becomes available. To enhance mission performance, TSA also facilitates both classified and unclassified briefings for industry representatives to ensure that the evolving threat picture is communicated to trade associations, industry executive leadership, and key industry security personnel. TSA's commitment to information sharing is strongly supported by two full-time threat intelligence sharing cells -the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) and the Surface Information Sharing Cell (SISC). Through these information sharing entities, TSA shares thousands of threat items, including cyber threat information. Additionally, we issue various cyber assessments and analytic products, including Cybersecurity Awareness Messages to operators and other products in conjunction with our sister component CISA and Federal law enforcement, to ensure widest distribution across the transportation sector. These two information sharing cells are excellent examples of government and industry partnership, and their establishment resulted directly from stakeholder collaboration. For instance, the SISC's establishment fulfills an important STSAC recommendation, and we continue working to enhance the SISC's capabilities.

Closing

Chairman DeFazio, Ranking Member Graves, and distinguished Members of the Committee, thank you for this opportunity to share the steps and measures TSA has taken in concert with our stakeholders to strengthen transportation critical infrastructure to address the serious and persistent cybersecurity threat. TSA is committed to ensuring appropriate security measures are in place to increase the cyber and physical security posture of our Nation's transportation systems. Thank you for the chance to appear before you today. I look forward to answering any questions you may have.