Statement of

Chad Gorman, Deputy Executive Assistant Administrator for Operations Support

Steve Lorincz, Deputy Executive Assistant Administrator for Security Operations

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

On

"Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector"

November 19, 2024

Washington, D.C.

Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Committee. My name is Chad Gorman, and I serve as the Deputy Executive Assistant Administrator for Operations Support within the Transportation Security Administration (TSA). I am joined today by Deputy Executive Assistant Administrator for Security Operations, Steve Lorincz. We appreciate the opportunity to appear before you today to discuss TSA's role in cybersecurity for our nation's transportation 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. In the years since 9/11, TSA has not only had to address the ever-present physical threats to aviation and surface transportation modes, but also dynamic and emerging cybersecurity threats to our nation's aviation, rail, highway and motor carrier, hazardous liquid, and natural gas pipeline infrastructure. 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, state, and local partners, including the Department of Transportation (DOT) as the Department of Homeland Security's (DHS) co-Sector Risk Management Agency for the Transportation System Sector.

Transportation Cybersecurity Threats

The August cyberattack at the Seattle-Tacoma International Airport serves as another reminder of the significant disruptions and broader impacts cybersecurity incidents can cause to transportation. Cyberattacks are an evolving and persistent threat. Cyber threat actors, including nation states, have demonstrated their intent and ability to conduct malicious cyber activity targeting critical infrastructure by exploiting vulnerabilities present in both Operational Technology (OT) (the hardware and software that controls physical devices, processes, and infrastructure) and Information Technology (IT) systems. Unlike traditional kinetic threats we confront, cyber threats are not bound by global borders. They can cross vast distances between our adversaries and U.S.-based critical transportation infrastructure in seconds, drastically impacting our ability to respond successfully with our more traditional and time-bound approaches. Nation state actors like Russia, China, Iran, and North Korea recognize cyber capabilities bypass geographical limitations and,

accordingly, they have developed and demonstrated capabilities that pose significant cyber threats to the United States The Director of National Intelligence has stated that our adversaries and strategic competitors possess, and in the case of the People's Republic of China (PRC), have prepositioned cyberattack capabilities that could be used against U.S. critical infrastructure, including transportation, especially during times of increased conflict.

This year, the Intelligence Community assessed that the PRC almost certainly could launch cyberattacks that could disrupt critical infrastructure within the United States, specifically highlighting oil and gas pipelines and rail systems. In May 2023, the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint Cybersecurity Advisory which highlighted for the first time a cyber threat cluster associated with the PRC identified as Volt Typhoon. There have been subsequent documents released on Volt Typhoon by CISA and other U.S. Government agencies. Volt Typhoon has been active since at least mid-2021 and targets U.S. critical infrastructure entities, including those in the transportation sector. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. government assesses with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks for disruptive or destructive cyber activity against U.S. critical infrastructure in the event of a major crisis or conflict with the United States. Observed behavior suggests Volt Typhoon intends to maintain access without being detected for as long as possible by relying almost exclusively on stealthy "living-off-the-land" techniques in which the cyber threat actor uses legitimate, built-in network administration tools to sustain, advance, and conceal an attack.

In April 2023, after receiving a briefing on the relevant intelligence, the Transportation Security Oversight Board (TSOB) recommended to TSA that a cybersecurity emergency exists that warranted the TSA Administrator's determination to expedite the implementation of critical cyber mitigation measures in aviation, which he had done through the exercise of his emergency regulatory authority by issuing Joint Emergency Amendment (EA) 23-01. Joint EA-2301 on March 7, 2023. The Joint EA amended the security programs for covered aviation entities to require performance-based cybersecurity measures intended to prevent the disruption and degradation of their critical systems. Additionally, in April of this year, President Biden extended the national emergency on malicious cyber-enabled activities, citing the continued significant and malicious activities that are posing an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

TSA is dedicated to protecting our Nation's transportation networks against evolving cyber 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 active information sharing within the federal government and with industry to reinforce the security posture of these networks.

Addressing Cybersecurity Threats Through Unique TSA Authorities

In response to these evolving threats, the TSA Administrator has utilized his emergency authorities found in both statute and regulation. In statute, Congress provided the TSA Administrator authority to issue regulations and security directives (SDs) immediately to protect transportation security. *49 U.S.C. §114(l)(2)).* In doing so, the Administrator may waive certain procedural requirements for traditional notice and comment rulemaking to carry out TSA's transportation security mission. SDs issued under this authority are subject to review by the Transportation Security Oversight Board (TSOB). The TSOB was established by the *Aviation and Transportation Security Act of 2001 (ATSA)* and consists of seven statutorily prescribed voting members, including DHS. DOT, Department of Justice, Department of Defense, Treasury Department, Office of the Director of National Intelligence, and National Security Council. The Board is chaired by the DHS Deputy Secretary. The TSOB is charged with reviewing and ratifying, or disapproving, any regulation or SD issued by the TSA Administrator under section 114(l)(2) within 30 days after the date of issuance. If a regulation or directive is not ratified by the TSOB, it may remain in effect for no more than 90 days. To date, the TSOB has reviewed and ratified all of TSA's surface cybersecurity SDs. The TSOB also has discretionary authority to review and make recommendations to the Administrator regarding transportation security plans. *(49 U.S.C. §115)(c)(5),(6)).* Under this authority, the TSOB provided its recommendation to TSA regarding a cybersecurity emergency warranting emergency action in the aviation sector.

By regulation, the TSA Administrator has the authority to issue emergency amendments to the security programs of regulated aviation operators. (*49 CFR §§1542.105, 1544.105, and 1546.105).* The Administrator may use this authority upon finding that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air commerce. The Administrator has additional regulatory authority to issue SDs to regulated aviation operators where it is determined that additional security measures are necessary to respond to a threat assessment or specific threat. (*49 CFR §§1542.303 and 1544.305.)*

The TSA Administrator's ability to leverage these authorities and respond immediately during emergency situations has significantly mitigated threats posed by a rapidly evolving, and increasingly volatile, cyber environment. The TSA Administrator's emergency authorities are essential and vital to the Nation's transportation security.

Examples of TSA's Cybersecurity Program

Immediately following a 2021 ransomware incident impacting a major US pipeline company, there was a clear understanding across the Administration, Congress, industry, and the public for the need to prevent future pipeline cybersecurity incidents. The Administration turned to TSA and the TSA Administrator leveraged his authority under 49 U.S.C. §114 to respond to emerging cyber threats by directing owners and operators of certain pipeline and natural gas facilities to implement a set of select cybersecurity protections to mitigate the threat. The TSA Administrator issued two SDs in 2021 to immediately address these threats. Among the many requirements, the SDs required pipeline companies to report cybersecurity incidents to CISA within 24 hours after they identify a cybersecurity incident; to designate a cybersecurity coordinator and alternate that is available to TSA around the clock; and to implement specific mitigation measures to protect against ransomware incidents.

Credible cyber threat information also supported the TSA Administrator's use of his emergency authority to implement additional security measures to U.S. surface (pipelines and railroads) and aviation (airports and air carriers) transportation networks. In regard to the surface transportation security domain, the cybersecurity SDs require higher risk pipelines, freight railroads, passenger rail, and rail transit operators to take several critical actions (rail transit operators only require the first three):

1. Develop and submit to TSA a Cybersecurity Implementation Plan (CIP) to achieve performance-based security outcomes;
2. Develop and maintain an up-to-date Cybersecurity Incident Response Plan (CIRP) to reduce the risk of operational disruption following cybersecurity incidents;
3. Develop and submit to TSA a Cybersecurity Assessment Plan (CAP) to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network and/or system vulnerabilities; and

4. Develop and submit to TSA an annual report that provides the results of the Cybersecurity Assessment Plan from the previous year.

Within aviation, the TSA Administrator used his regulatory authority to amend established security programs of the nation's largest air carriers and airports to include cybersecurity. Like the surface SDs, these amendments started with requirements to designate a Cybersecurity Coordinator, report cybersecurity incidents to CISA, and to develop a CIRP. They now also include requirements to develop a CIP and CAP and to allow TSA to inspect these documents.

In promulgating these SDs and security program amendments, TSA engaged with stakeholders to enhance understanding of the threat landscape and gather industry feedback. This included stakeholder discussions at the CEO-level with DHS and TSA leadership, classified threat briefings for industry, multiple policy reviews by industry and government stakeholders, and consistent engagement sessions with transportation associations and regulated entities for awareness on the proposed strategies. Through these regular engagements with industry partners, we quickly learned that our initial approach to cybersecurity in surface modes was too prescriptive. This approach limited innovation and hindered industry's ability to quickly respond to evolving and emerging dynamic cyber threat landscapes. Based on that feedback, TSA quickly transitioned our regulatory framework in 2022 to an outcome focused, performance-based model that remains our model to the present day in both surface and aviation modes. This rapid shift to performance based SDs versus prescriptive SDs demonstrates the flexibility of TSA's emergency authorities and highlights the power of collaboration with our industry partners to collectively address security issues with measures tailored to specific transportation environments.

Since August 2023, TSA also led several in-person and virtual meetings to discuss the pipeline SDswith pipeline owners and operators from various associations and companies. Additionally, TSA hosts a bi-weekly call with the owners and operators subject to the rail SDs to share information and answer questions on the SDs and inspection requirements. Similar calls have begun within the last few months for airports and air carriers. In these engagements, TSA also discusses its cybersecurity policy and strategy, identifies opportunities for improvement, and provides contextual information via the sharing of intelligence and incident information.

Finally, TSA also engages regularly with TSA's Surface Transportation Security Advisory Committee (STSAC) and the Aviation Security Advisory Committee (ASAC) to share and discuss security requirements, issues, and challenges. These statutorily created committees

include representation from the interagency and industry. Whenever able, we will continue to engage with industry partners prior to issuing new security requirements.

Concurrently with these efforts, TSA published a Notice of Proposed Rulemaking (NPRM) that would codify the provisions of the SDs for certain surface modes of transportation into a Cybersecurity Risk Management Program. This proposed rule opened for public comment on November 8, 2024. It continues TSA's commitment to performance-based requirements, builds on TSA's previously issued cybersecurity requirements from the SDs and seeks to establish a sustainable and comprehensive cyber risk management program for owners and operators that have higher cybersecurity risk profiles. Our routine engagements with stakeholders, as well as coordination with inter-agency partners such as DOT, USCG, and CISA, have been critical in this process – as with the SDs, their feedback has informed decisions on the proposed rulemaking.

Within the aviation sector, TSA continues to partner with aviation entities on elevating their cybersecurity stance. TSA has partnered and communicated, at the appropriate level based on the maturity of the covered parties, cybersecurity program changes to their cybersecurity programs. As of October 1, 2024, TSA has reviewed and approved over 70 percent of the cybersecurity implementation plans and conducted several inspections of covered parties.

Within the surface modes, all pipeline CIPs have been approved, and nearly all rail plans have been approved. In preparation for the SD CIP inspections, owners and operators were contacted by their Regional Security Director or inspection point of contact well in advance of the inspection to provide details and to coordinate any documentation in advance to ensure all parties were properly prepared. As of May 2024, TSA completed all initial pipeline inspections. By the end of Fiscal Year (FY) 2024, 96 percent of rail inspections have been conducted.

With the approved CIPs in surface, most owners and operators have developed and submitted their CAPs to test the effectiveness of the measures outlined within their CIPs. As of October 23, 2024, TSA has approved 99 percent of pipeline and 45 percent of rail CAPs.

Information Sharing and Engagement

Our work does not simply end after issuing these cybersecurity requirements. On the contrary, TSA continues its robust stakeholder engagement to mitigate cyber threats. We work closely with covered owners and operators to successfully implement these requirements, educate our vast network of transportation owners and operators, and continue to seek input from both the

STSAC and the ASAC on how to best integrate cybersecurity into the fabric of our transportation security mission. TSA conducts extensive outreach with thousands of individual transportation owners and 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.

On behalf of DHS, TSA and USCG are each a Co-Sector Risk Management Agency for the TSS along with the DOT. In this role, TSA serves with the USCG as the executive agents 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 systems sector.

Under the proposed CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule published on April 4, 2024, all entities within the TSS—that are currently required to report to TSA—will also be required to report to CISA. The proposed rule is in line with TSA's SDs and security programs that require certain transportation entities to report cybersecurity incidents, as defined by TSA, to CISA within 24 hours of identification. Regulated entities complying with TSA's requirements will not need to make a duplicate report to CISA; all TSA reporting requirements will occur via a report from TSA into CISA's own systems. Although CIRCIA requirements do not limit TSA's authority to impose cybersecurity reporting requirements, define reportable incidents more broadly than CISA, or impose a timeframe for reporting that is shorter than the timeframe required by CIRCIA, TSA has ensured that cybersecurity reporting is integrated with the system under development by CISA.

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 facilitates both classified and unclassified briefings for trade associations, industry executive leadership, and key industry security personnel representatives to ensure full understanding of the evolving threat picture. As previously stated, TSA's commitment to information sharing with industry is strongly supported by two full-time threat intelligence sharing cells—the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) and the Surface Intelligence Sharing Cell (SISC). Through these entities, TSA shares thousands of threat items, including cyber threat intelligence with cleared stakeholders. These two intelligence sharing cells are excellent examples

of government and industry partnership, and their establishment resulted directly from stakeholder collaboration. Close collaboration with our public and private partners will continue to inform TSA's next steps in the cybersecurity arena.

Finally, we would like to thank Congress and this Subcommittee for your support of TSA's transportation security mission and securing the funding for critical cyber resources in FY 2024. The FY 2025 President's Budget Request, if enacted, will fund specially trained personnel to accelerate cybersecurity inspection and compliance efforts across the entire TSS. TSA will use the funding to emphasize aviation and surface sector resiliency, use of cyber-tools, a trained cyber response staff, a cyber analytical staff, and a regulatory support staff. We recognize the continued need to recruit, train, and retain cybersecurity professionals within TSA. Through recruitment and retention incentives, to include supporting cybersecurity development training opportunities and cybersecurity certifications for personnel, we continue to build our cybersecurity workforce, positioning TSA to effectively tackle the evolving cybersecurity threat as supported by recent budget requests.

Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee, 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 cybersecurity defenses of our Nation's most critical transportation systems. I look forward to answering any questions you may have.