MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

March 6, 2025

Mr. Adam Stahl
Acting Administrator
Transportation Security Administration
6595 Springfield Center Drive
Springfield, VA 20598

Dear Acting Administrator Stahl:

The Committee on Homeland Security is committed to ensuring the security, resilience, and operational continuity of our nation's transportation systems, which serve as the foundation of the American economy, facilitate the daily movement of millions of passengers, and sustain the flow of goods that support both commerce and national security. As cyber threats targeting transportation infrastructure continue to evolve in scale and sophistication, it is imperative that the Transportation Security Administration (TSA) maintain an adaptive cybersecurity posture to safeguard against these evolving risks.

Within the broader framework of the Department of Homeland Security's (DHS) role as the Co-Sector Risk Management Agency (Co-SRMA) for the Transportation Systems Sector,[1] TSA is responsible for securing aviation and surface transportation systems against both physical and cyber threats.[2] This interagency construct underscores the necessity of a coordinated, whole-of-government approach to mitigating cyber risks across commercial and general aviation, mass transit systems, freight and passenger rail, and pipeline networks.

Recent cyber incidents and information technology (IT) disruptions have exposed systemic vulnerabilities within critical transportation systems and networks, reinforcing the urgency of enhanced security and resilience measures. The global IT outage on July 19, 2024, caused by a faulty software update from CrowdStrike, disabled approximately 8.5 million

[1] Federal agencies with a lead role in assisting and protecting one or more of the nation's 16 critical infrastructures are referred to as sector risk management agencies (SRMA). SRMAs are federal departments or agencies, designated by law or presidential directive, with specific responsibilities for their designated critical infrastructure sectors. *See* 6 U.S.C. § 651(5). The Department of Homeland Security is a co-SRMA for multiple sectors, including the Transportation Systems Sector.

[2] 49 U.S.C. §114(l)(2); *see also* "*Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector*": Hearing Before the Subcomm. on Transportation and Maritime Security of the H. Comm. on Homeland Sec., 118th Cong., (Nov. 19, 2024), (statement of Chad Gorman, Deputy Executive Assistant Administrator for Operations Support, TSA; Steve Lorincz, Deputy Executive Assistant Administrator for Security Operations, TSA).

Windows systems, severely disrupting airlines, rail networks, financial institutions, hospitals, and emergency services worldwide, with financial losses estimated to exceed $10 billion.[3]

Just weeks later, in August 2024, a cyber incident at Seattle-Tacoma International Airport disrupted TSA screening operations, further highlighting the direct impact of cyber threats on frontline aviation security.[4] Beyond these incidents, the persistent activities of foreign adversaries, including the People's Republic of China (PRC) cyber actor known as Volt Typhoon, pose an enduring risk to U.S. transportation infrastructure.[5] State-sponsored cyber actors have demonstrated a deliberate and sustained effort to infiltrate and pre-position themselves within critical networks, potentially enabling disruptive or destructive operations in times of geopolitical conflict.

While these recent events have drawn national attention, the systemic risks facing U.S. transportation infrastructure are not new. The 2021 Colonial Pipeline ransomware attack served as an early warning, demonstrating how a single cyber intrusion could disrupt fuel distribution along the East Coast, resulting in widespread operational and economic consequences.[6] That incident prompted a paradigm shift in the TSA's cybersecurity posture. In response, TSA undertook an unprecedented expansion of cybersecurity regulatory efforts in the surface transportation sector, issuing mandatory cybersecurity directives across the pipeline and rail industries for the first time in the agency's history.[7] These directives, which establish requirements for threat reporting, incident response, and mitigation measures, represent a significant departure from TSA's traditionally voluntary and collaborative approach.[8]

Moreover, TSA's Notice of Proposed Rulemaking (NPRM) published on November 6, 2024, entitled, "*Enhancing Surface Cyber Risk Management*," would further mandate the establishment of cyber risk management programs for certain pipeline and rail operators, extending cybersecurity resilience efforts across higher-risk transportation stakeholders.[9] According to the NPRM, the proposed rule aims to formalize TSA's existing cybersecurity directives while incorporating the cybersecurity framework developed by the National Institute of Standards and Technology (NIST) and the cross-sector cybersecurity performance goals

---

[3] Colby L. Pechtol et al., *CrowdStrike IT Outage: Impacts to Public Safety Systems and Considerations for Congress*, Congressional Research Service, December 4, 2024, https://crsreports.congress.gov/product/pdf/IF/IF12717.
[4] Lauren Girgis, *Sea-Tac Airport cyberattack caused by global ransomware gang, Port says*, Seattle Times, September 13, 2024, https://www.seattletimes.com/life/travel/sea-tac-cyberattack-caused-by-global-ransomware-gang-port-says/.
[5] Cybersecurity and Infrastructure Security Agency (CISA), *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Target U.S. Critical Infrastructure* (AA24-038A), February 7, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.
[6] David E. Sanger et al., *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES, May 13, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
[7] Press Release, U.S. Dep't of Homeland Sec., *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators* (May 27, 2021), https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.
[8] *Id.*
[9] 89 Fed. Reg. 88488 (Nov. 7, 2024); *see* https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management

established by the Cybersecurity and Infrastructure Security Agency (CISA).[10] With the public comment period closing on February 5, 2025, evaluating the rule's potential impact on security, regulatory compliance, and industry operations should be a priority.[11]

As TSA refines its cybersecurity posture, it is also essential to assess whether this regulatory framework is effective, sustainable, and appropriately balanced between security imperatives and operational realities. TSA must ensure that its cybersecurity framework is not only effective but also agile enough to respond to multiple simultaneous cyber incidents that impact different nodes of the transportation sector without compromising operational continuity. We are concerned that the Biden administration did not take this pragmatic and balanced approach to regulation for the Transportation Systems Sector, instead imposing more requirements on entities that already face a complex cyber regulatory landscape. A rigid or overly burdensome approach could impose operational challenges, while insufficient oversight may leave critical vulnerabilities unaddressed. Striking the right balance will require continuous engagement with industry partners, regular assessments of existing directives, and the flexibility to refine policies in response to emerging threats and technological advancements.

To better understand TSA's cybersecurity framework and its implementation across the transportation sector, we respectfully request responses to the following questions by no later than March 27, 2025:

1. How many personnel within TSA's Surface Policy Division, under the Policy, Plans, and Engagement Office within Operations Support, are dedicated to cybersecurity efforts? Additionally, how many TSA employees across the agency possess technical cybersecurity expertise, and how is TSA's cybersecurity workforce structured to address risks across aviation, rail, and pipeline infrastructure?

2. What public-private sector partnerships does TSA maintain or leverage when developing rules, frameworks, or trainings?

3. What feedback has TSA received from industry stakeholders regarding the November 6, 2024, cybersecurity NPRM and other cyber-related requirements, and what steps has TSA taken to address their concerns?

4. In what ways has TSA collaborated with CISA to ensure alignment and harmonization of proposed cybersecurity regulations and requirements?

---

[10] Press Release, Transportation Sec. Adm., *TSA announces proposed rule that would require the establishment of pipeline and railroad cyber risk management programs* (Nov. 6, 2024), https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and.

[11] *Id* at 11.

5. What specialized training, continuous education, and readiness initiatives are in place to ensure TSA personnel remain ahead of emerging cyber threats, including those posed by nation-state actors such as Volt Typhoon?

6. What tools, methodologies, and technologies does TSA employ to detect, deter, and respond to cyber intrusions targeting transportation infrastructure? How does TSA ensure real-time monitoring of cyber threats across multiple sectors?

7. What is TSA's formal incident response framework for large-scale cyberattacks affecting multiple transportation sectors simultaneously and how does TSA coordinate with federal agencies and industry stakeholders to ensure a swift and effective response?

8. Given reports that adversarial nation-state actors, including Volt Typhoon, have infiltrated U.S. critical infrastructure networks, what specific measures is TSA implementing to identify, neutralize, and prevent pre-positioned cyber threats within transportation systems?

9. What actions is TSA taking to mitigate cybersecurity risks associated with third-party software providers and supply chain vulnerabilities, particularly in transportation sectors heavily reliant on external vendors?

10. How is TSA leveraging emerging technologies, including artificial intelligence, automation, and quantum computing, to enhance cybersecurity protections? What potential risks do these technologies pose, and how is TSA mitigating them?

11. Given TSA's shift toward mandatory cybersecurity directives, does the administration support the continuation of this regulatory approach? If not, what changes does the administration intend to make regarding TSA's cybersecurity regulations for the transportation sector?

12. How does TSA evaluate whether the security directives and any other regulatory measures issued since 2021 have been effective? Are there plans to reassess or adjust the regulatory approach based on industry feedback and operational challenges?

Should any of these matters require discussion or disclosure in a classified setting, the Committee stands ready to arrange a secure briefing.

Under Rule X of the U.S. House of Representatives, the Committee on Homeland Security is the principal committee of jurisdiction for overall homeland security policy and has special oversight of "all Government activities relating to homeland security, including the interaction of all departments and agencies with the Department of Homeland Security."

Thank you for your attention to this important matter and your prompt reply.

Sincerely,

MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security

CARLOS A. GIMENEZ
Chairman
Subcommittee on Transportation
and Maritime Security

ANDREW R. GARBARINO
Chairman
Subcommittee on Cybersecurity and
Infrastructure Protection

SHERI BIGGS
Member of Congress

Encl.

cc: The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security

The Honorable LaMonica McIver, Ranking Member
Subcommittee on Transportation and Maritime Security

The Honorable Eric Swalwell, Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection