

United States Senate

January 3, 2022

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Washington, DC 20528

The Honorable Pete Buttigieg
Secretary of Transportation
Washington, DC 20590

Dear Secretary Mayorkas and Secretary Buttigieg:

We write to request information on the implementation of the U.S. Department of Homeland Security (DHS) and U.S. Department of Transportation's (DOT) responsibilities as Co-Sector Risk Management Agencies (co-SRMAs) for the nation's critical transportation infrastructure. In anticipation of increasing cybersecurity threats to transportation systems, DHS and DOT must have the capabilities and resources to prevent and address these threats. As such, we request information about DHS and DOT's security-related processes to detect, prevent, and respond to cyber threats, including the responsibilities of each component agency under the Transportation Systems Sector-Specific Plan to secure the nation's critical infrastructure.

Cyberattacks on American transportation infrastructure are escalating in frequency and severity, as evidenced by the ransomware attack earlier this year on Colonial Pipeline, one of the nation's largest pipelines, which led to the shutdown of a network that carries nearly half the gasoline, diesel, and jet fuel for the East Coast. At the same time, many state and local transit agencies are not fully equipped to implement more than basic cybersecurity protections. In fact, a study by the Mineta Transportation Institute found that only 60% of transit agencies had a cybersecurity plan in place last year.¹ Nevertheless, other entities in the extensive and diverse transportation sector, which includes aviation, highways, motor carriers, maritime transportation, railroads, rail transit, and pipelines, have been implementing comprehensive cybersecurity plans for decades in collaboration with Federal agencies. As such, federal efforts to ensure that our nation is properly prepared to address cybersecurity threats to the transportation system require a delicate balance to provide critical assistance to entities that need new or additional cybersecurity support, while recognizing effective practices that some entities already have in place.

In 2013, Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure and Resilience*, identified the transportation system as one of sixteen critical infrastructure sectors and designated DHS and DOT as co-SRMAs.² We recognize that DHS and DOT have the complex and enormous responsibility of ensuring the security and resilience of the nation's transportation

¹Scott Belcher, Terri Belcher, Eric Greenwald, Brandon Thomas, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, San Jose State University, Mineta Transportation Institute (September 2020), <https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf>

² Presidential Policy Directive – Critical Infrastructure Security and Resilience, (2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

systems, supporting the systems' ability to quickly, safely, and securely move people and goods throughout the country and overseas.

With this in mind, we request information about how DHS and DOT are meeting their six responsibilities as co-SMRAs, recently delineated by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Division H, Title 90, section 9002):

- Support risk sector management,
- Assess sector risk,
- Sector coordination,
- Facilitating information sharing of information regarding physical security and cybersecurity threats within the designated sectors or subsectors,
- Supporting incident management, and
- Contributing to emergency preparedness efforts

Additionally, please provide an update on how DHS and DOT collaborate to avoid both gaps and redundancies in Federal risk management including specific roles for each agency and delineation of law enforcement and safety responsibilities.

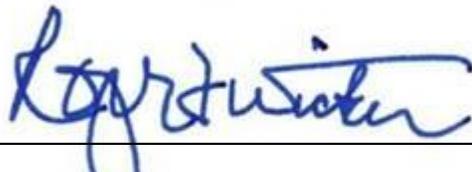
Finally, while the Transportation Systems Sector-Specific Plan from 2015 is a helpful tool, the nature of risk to our critical infrastructure has changed over the past six years. Our society and economy are increasingly dependent on computer networks and information technology solutions. Ransomware attacks on the transportation industry, just one derivative of cyber-attacks, increased by 186% between June 2020 and June 2021.³ Therefore, we request information on any efforts to update the Transportation Systems Sector-Specific Plan to provide the most effective assistance possible to improve the security and resilience posture of the nation's transportation system.

Thank you for your attention to this important matter. We look forward to your reply and continuing to work with you to keep the nation's infrastructure secure.

Sincerely,



Jacky Rosen
United States Senator

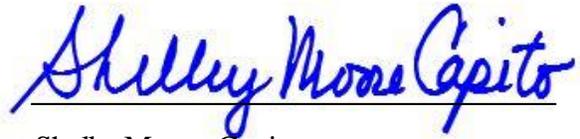


Roger F. Wicker
United States Senator

³ *Ransomware Attacks on the Transportation Industry*, CyberTalk.org (July 2021), <https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/>



Rob Portman
United States Senator



Shelly Moore Capito
United States Senator



Reverend Raphael Warnock
United States Senator



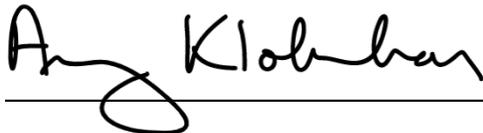
Todd Young
United States Senator



Dan Sullivan
United States Senator



James Lankford
United States Senator



Amy Klobuchar
United States Senator



Margaret Wood Hassan
United States Senator