COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Transportation & Maritime Security Subcommittee Ranking Member Shri Thanedar (D-MI)

Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector

November 19, 2024

The May 2021 ransomware attack against Colonial Pipeline served as a major turning point in TSA's approach to securing transportation systems from cyber attacks.

Prior to the attack, TSA's efforts to ensure the cybersecurity of transportation systems relied largely upon voluntary cooperation and adoption of recommended guidelines and best practices.

The attack had far-reaching impacts, as Colonial Pipeline shut down the transportation of fuel through the pipeline, which services much of the Southeastern United States.

The public flocked to gas stations, leading to long lines and fuel shortages.

In the aftermath of the attack, TSA assumed a more regulatory posture towards transportation cybersecurity, acting quickly to issue the first-ever cybersecurity directives for pipeline systems and facilities.

TSA followed that initial security directive with similar mandates for owners and operators of freight rail, passenger rail, and public transit systems, as well as changes to security programs for airports and air carriers.

TSA required owners and operators to adopt essential cybersecurity measures, such as designating a cybersecurity coordinator and reporting cyber incidents.

TSA engaged extensively with industry stakeholders and quickly learned that its mandates were viewed as too prescriptive and inflexible.

To provide regulated parties with enough flexibility to innovate and respond to evolving threats, TSA developed a novel approach in subsequent directives, focusing on desired performance and security outcomes rather than specific measures.

Over the past couple years, TSA has continued to refine its approach through extensive engagement with stakeholders.

Earlier this month, TSA issued a notice of proposed rulemaking to codify cybersecurity requirements for owners and operators of pipeline, rail, and over-the-road bus systems.

TSA's proposal, which is currently open for comment, would require system owners and operators to establish and execute a comprehensive cyber risk management program, representing a significant step forward in the evolution of TSA's cybersecurity efforts.

The maturation of those efforts is also reflected in recent adjustments to TSA's investment in cybersecurity.

In Fiscal Year 2021, prior to the Colonial Pipeline attack, Congress funded TSA's cybersecurity activities at $86 million, with 86 dedicated positions.

Now, in Fiscal Year 2024, that investment has increased to $137 million and 167 positions.

For Fiscal Year 2025, the Biden-Harris Administration has requested an additional increase of $8 million and 41 positions.

I hope Congress will continue to support TSA's efforts to enhance the cybersecurity of the transportation sector.

To those who may question the need for regulations or TSA's use of emergency security directives, I would note that, if TSA continued to rely on voluntary compliance with recommended guidelines and another attack like the attack on Colonial Pipeline were to occur, the public would rail against both TSA and Congress for allowing a disproven approach to continue.

Our adversaries are continuing to adapt and pursue offensive cyber capabilities; now is the time for TSA and its partners to ensure our security defenses are fully fortified.

# # #

Media contact: Adam Comis at 202-225-9978