COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Securing U.S. Surface Transportation from Cyber Attacks

Joint Hearing – the Subcommittee on Transportation and Maritime Security and the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation

February 26, 2019

Since the 9/11 attacks, the U.S. government has focused on closing gaps in physical aviation security by Federalizing passenger and baggage screening, hardening cockpit doors, and deploying improved screening technologies and training.

In September 2018, the subcommittees held a joint hearing highlighting the potential harm from an important, underdiscussed vector: cyber threats to aviation. Today, we will provide the same attention to cybersecurity threats to the surface transportation sector.

With TSA dedicating most of its resources to protecting aviation, the surface transportation sector—including freight and passenger trains, commuter rail, mass transit, buses, and pipelines—presents a relatively soft target for mass-casualty attacks. We rely on these diverse assets not only support for our personal and business travel, but also commercial shipping, the transport of natural gas, and a host of other activities essential to the health of our economy and national security.

In recent years, surface transportation systems overseas have been hit by terrorist attacks. On our own shores, New York City's subway was the target of a failed terrorist plot in December 2017. Given the level of risk to surface transportation, I am concerned that we have not sufficiently protected this sector against cyber threats.

To date, no cyberattacks have disrupted the actual operations of surface transportation systems, but attacks have resulted in financial disruption and affected public confidence in various modes of surface transportation. These small-scale attacks have shown that a relatively simple intrusion could upend surface transportation services, causing significant harm and disruption.

Last year, Congress established Cybersecurity and Infrastructure Security Agency, or CISA, as the operational agency within the Federal government charged with serving as the primary civilian interface for cybersecurity information sharing. CISA will continue to play a critical role in providing cybersecurity resources within DHS, including to TSA, and to industry to combat cyber threats to critical infrastructure.

TSA, for its part, maintains responsibility for the security of all modes of transportation.

Working together within DHS, CISA and TSA are uniquely positioned to address cyber threats to transportation.

I would note that DHS's authorities and capabilities across all critical infrastructure sectors and all modes of transportation makes it better positioned to secure pipelines than the Department of Energy, despite some suggestions to the contrary.

In December 2018, in coordination with CISA, TSA released its first-ever Cybersecurity Roadmap, providing a vision for the future of cybersecurity across all modes of transportation.

While DHS is headed in the right direction, much work remains. In many cases, surface transportation sector owners and operators struggle with the same cyber challenges that plague other industries: a national shortage of skilled cybersecurity personnel, a workforce with minimal cybersecurity training and awareness, and resource constraints across the board.

Owners and operators must also address supply chain concerns, including those posed by the emergence of a Chinese state-owned enterprise manufacturing subway cars for U.S. mass transit systems. Government and industry must work together to ensure that cyber threats and vulnerabilities are fully understood and appropriately addressed.

Finally, at a hearing on surface transportation security, I would be remiss if I did not point out that TSA remains non-compliant with requirements to publish surface transportation security regulations, which were enacted over a decade ago in the Implementing Recommendations of the 9/11 Commission Act of 2007.

The rules required under the law would help TSA to better assess and address vulnerabilities within the surface transportation sector, including cybersecurity vulnerabilities.

I look forward to hearing from this panel of witnesses today, and I hope they will give us a candid assessment of the cybersecurity posture of our surface transportation sector.

# # #

Media contact: Adam Comis at (202) 225-9978