COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Transportation and Maritime Security Subcommittee Chairman Lou Correa (D-CA)

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

We have a great panel of distinguished Members on both sides of the aisle, and I look forward to working with you all to tackle the security challenges facing the transportation and maritime sectors. I am glad to hold our first hearing jointly with the Cybersecurity Subcommittee and its leaders, Chairman Richmond and Ranking Member Katko. I am also happy to welcome our two panels of witnesses today. We look forward to your testimony.

We are here today to discuss an important topic: the cybersecurity of our nation's mass transit, rail, pipeline, and other surface transportation systems. Cyber threats are a growing concern for security experts across many sectors—and the surface transportation sector is no different. Millions of Americans rely on surface transportation every day for critical services, and an attack against a large subway system or pipeline could have a hugely negative impact.

Government and industry have both struggled to address cyber threats, which are evolving quickly and becoming more complex. However, I believe DHS is well positioned to lead cybersecurity efforts across critical infrastructure sectors, including the surface transportation sector.

Last year, Congress established the Cybersecurity and Infrastructure Security Agency, or CISA, making clear its status as the preeminent cybersecurity agency within the Federal government. To secure surface transportation from cyber attacks, CISA works closely with TSA, which is responsible for securing all modes of transportation.

In December 2018, working with CISA, TSA released a Cybersecurity Roadmap, which sets priorities for securing transportation from cyber threats. The publication of this roadmap is an important step in addressing the cybersecurity of transportation, but it must be followed by concrete action.

In the surface mode, TSA works collaboratively with the system owners and operators who provide frontline security at the local level. In coordination with CISA, TSA must ensure owners and operators have access to the resources, intelligence, guidelines, and assessments needed to ensure the cybersecurity of their systems.

Government and industry stakeholders together must also address supply chain security concerns. We must make sure that surface transportation systems are not made vulnerable to cyber espionage due to unchecked foreign manufacturing of subway cars or other infrastructure.

Finally, some have questioned whether DHS has paid enough attention to pipeline security and have raised the idea of moving responsibility for securing pipelines to another department. Doing so would be foolhardy and go against the reasons Congress established DHS, TSA, and CISA. Only DHS has the scope of authorities and access to intelligence needed to address cyber threats across critical infrastructure sectors.

For example, only TSA has authority to issue Security Directives to require immediate implementation of security measures across or within modes of transportation in the face of an imminent threat or ongoing attack.

DHS has made significant progress in securing pipelines, including recent updates to TSA's Pipeline Security Guidelines, and it should be allowed to build upon its ongoing efforts.

This hearing provides a great opportunity to discuss the work of both government and private industry to secure all modes of transportation from cyber threats, and I look forward to a productive conversation.

# # #

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