COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Joint Subcommittee Hearing Statement of Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Chairwoman Yvette Clarke (D-NY)

Transportation Cybersecurity: Protecting Planes, Trains, and Pipelines from Cyber Threats

October 26, 2021

We are here today to assess the Administration's actions aimed at mitigating the cybersecurity challenges facing the transportation sector. Earlier this year, our Subcommittees worked together to evaluate how the Federal government partnered with the private sector to respond to a ransomware attack against Colonial Pipeline, which resulted in 5,500 miles of pipeline being shut down.

As panic led to fuel shortages at gas stations along the East Coast and airlines scrambled to find alternative fuel supplies, we learned that: attackers infiltrated Colonial Pipeline's business network using a legacy VPN that did not require multi-factor authentication; the flow of information between Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency, and the Transportation Security Administration was slow, fueled in part by ongoing confusion about which agency was in charge; and despite repeated offers from TSA, Colonial Pipeline had not yet undergone an important security assessment - a Validated Architecture Design Review - and did not have a disaster response plan that contemplated the full scope of cyber threats.

Shocked by what we learned during their oversight of Colonial Pipeline and other recent high-profile cyber incidents, Members of Congress have begun to question whether the Federal government's approach to cybersecurity - which relies primarily on voluntary partnerships – actually works, or whether some security requirements ought to be mandated. The notion that certain entities should be subject to cybersecurity standard mandates is not new.

Almost ten years ago, President Obama issued Executive Order 13636, on Improving Critical Infrastructure Cybersecurity. The Executive Order directed sector risk management agencies to evaluate whether they had sufficient authority to establish cybersecurity requirements for critical infrastructure entities for which a "cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security" – and report back to DHS and the White House with what they found. To the best of my knowledge, no agency suggested they lacked authority to issue such requirements.

Nevertheless, for nearly a decade, the Federal government has continued to pursue security policies that relied primarily on voluntary partnerships with the private sector. That's why the security directives that TSA issued for pipelines - and the requirements TSA plans to issue for rail, transit, and aviation - deserve such careful attention. They mark a pivotal transition in the Federal government's approach to cybersecurity.

As a representative from Brooklyn, I welcome TSA's renewed interest in improving the cybersecurity posture of the transportation sector. New York City is a transportation hub – home to two major airports, several rail lines, and the largest mass transit system in the country. Just six months ago, hackers reportedly tied to the Chinese government breached Metropolitan Transportation Authority's

network. Fortunately, they did not gain access to operational systems that control rail cars – but I remain concerned about the cybersecurity of mass transit systems, generally, and MTA's network, in particular. Given the degree to which middle- and low-income people rely on public transportation, a cyberattack affecting mass transit could have a disproportionate impact on these populations.

In light of the conversations I have had regarding cybersecurity threats to rail and aviation, I also support TSA's efforts to raise the bar on cybersecurity for these subsectors. That said, as the Federal approach to securing critical infrastructure evolves, we must get it right. TSA's security directives on pipelines - and pending security directives on transit, rail, and aviation - present an opportunity to better understand the Administration's security goals, how the security directives align with those goals, and the private sector's ability to effectively implement the directives.

Today, I hope to identify the lessons learned from the rollout and implementation of the pipeline security directives, so we can use them to inform future transportation security directives to ensure that they are buying down risk and yielding the security benefits we expect. More broadly, I hope today's conversation will provide insight into how we can raise the cybersecurity posture across critical infrastructure sectors.

# # #

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