COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

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

October 26, 2021

Today's hearing occurs amid a shifting conversation on how to secure our Nation's transportation systems from cyber attacks. The Transportation Security Administration has long relied on voluntarily collaboration with industry partners to develop and implement cybersecurity measures. The ransomware attack on Colonial Pipeline and the ensuing gas shortage earlier this year tested the effectiveness of this approach and highlighted the devastating potential effects of a successful cyber attack on transportation systems.

In the aftermath of the attack, the Biden Administration moved swiftly to mandate cybersecurity requirements for owners and operators of critical pipelines through two security directives issued by the TSA, with support from CISA. Over time, TSA will replace these security directives with full notice-and-comment regulations, marking the start of a new regulatory scheme for securing the transportation sector from cyber attacks.

Earlier this month, Secretary Mayorkas announced that TSA will also expand this mandatory approach to other modes of transportation by issuing new cybersecurity requirements for rail, transit, and aviation. Indeed, while the attack on Colonial Pipeline dominated the headlines, it is far from the only recent cyber attack we have seen targeting transportation systems. From the subway system in New York City to the Port of Houston, we have seen cyber attacks attempted across all modes of transportation.I commend the Biden Administration for taking the bold steps needed to address these emerging threats.

As DHS embarks upon this new approach, it must act deliberately to ensure its mandates deliver the intended security results. First, TSA must work in close collaboration with CISA and industry experts to develop requirements that are intelligence-based, actionable, and crafted to achieve the greatest security benefit. TSA must focus its enforcement efforts on desired outcomes and work with stakeholders to provide flexibility in how regulated parties achieve those outcomes.

Second, DHS must develop a plan for developing the cybersecurity expertise and resources it will need at TSA and CISA to carry out robust outreach and enforcement efforts—not just for the immediate implementation of new requirements, but as a regular way of doing business going forward. Congress will need to fully fund these efforts, and I look forward to working with my colleagues to deliver the necessary resources.

Finally, as DHS considers plans for securing other critical infrastructure sectors from cyber attacks, the transportation sector may serve as a model for the prospect of mandating cybersecurity measures. DHS must be transparent with Congress, stakeholders, and the public about its successes and failures.

# # #

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