COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Joint Subcommittee Hearing Statement of Transportation & Maritime Security Subcommittee Chairwoman Bonnie Watson Coleman (D-NJ)

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

October 26, 2021

I want to be crystal clear: when it comes to transportation cybersecurity, inaction isn't an option. When gas stops flowing due to a cyberattack, it doesn't just impact the pipeline's owner. It means Americans struggle to fill up their tanks. If hackers succeed in bringing down a plane or derailing a train, it's not an airline or railroad that would pay the steepest price. The real cost would be borne by the passengers injured or killed. Simply put, when you own critical infrastructure, people's lives and livelihoods depend on your cybersecurity. Yet despite the stakes, most transportation operators currently have no obligation to meet even baseline cybersecurity standards.

The status quo is dangerous. We're all familiar with the attack on Colonial Pipeline, but just this year, hackers have also targeted New York's MTA, the Massachusetts ferry system, the Port of Houston, one of the largest depositories of airline passenger records, a leading pipeline maintenance company, and global freight railroads. The list goes on. Unquestionably, our Nation's transportation systems are facing a crisis. Fortunately, TSA has begun the process of requiring critical operators to take basic cybersecurity precautions.

The recent cyber security directives for pipelines – and Secretary Mayorkas' announcement of forthcoming requirements for rail, transit, and aviation – are justified, necessary, and an important first step. But more action is needed. For instance, TSA must ensure all transportation modes are covered. Particularly as vehicles become increasingly connected and autonomous, the cybersecurity of motor-carriers and buses cannot be forgotten. Meanwhile, the Coast Guard needs to hold ferries, ports, and other maritime systems to similar standards.

There's also the question of implementation and enforcement. If an operator proposes an alternative procedure that maintains robust cybersecurity, TSA needs to provide timely, substantive feedback. By the same token, if operators fail to comply – leaving our Nation's critical infrastructure vulnerable to attack – TSA must have the resources to enforce the rules. And ultimately, TSA should pursue traditional notice-and-comment regulations so stakeholders can offer meaningful input. But these conversations around implementation shouldn't distract from a fundamental fact: there's no substitute for mandatory transportation cybersecurity requirements, like those announced by TSA and Secretary Mayorkas.

While many operators employ best practices, invest in cybersecurity talent, and coordinate with government voluntarily, some cut corners and put us all at risk. Without requirements, there is nothing to compel those companies to improve. That's a prospect we cannot take lightly, because in the 21st Century, physical security and cybersecurity are two sides of the same coin. Historically, to hijack a plane, you had to clear TSA's checkpoint and then breach the cockpit. Today, it may be possible to hijack a plane by hacking it. The same is true for railroads, subways, and other modes. Cameras and guards are no match for a hacker seeking to control or derail a train.

This isn't science fiction. This is the future, and cybersecurity requirements for all modes are the way to prepare for it, as well as tackle today's immediate threats – such as ransomware and state-sponsored data theft. A recent study found that only 60% of transit agencies have a cybersecurity preparedness program in place, and the surge in cyberattacks against railroads, airlines, airports, and maritime assets suggests an equally grim picture in those modes.

This is our moment to ensure that every transportation operator in America prepares themselves for 21st Century threats. We can't wait until a hacked plane falls from the sky or a breached railroad gridlocks our Nation's supply chain to take action. I look forward to hearing from our panel today about what can be done to shore up the cyber defenses of our transportation systems.

# # #

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