Senate Committee on Commerce, Science, & Transportation
Hearing on "Pipeline Cybersecurity: Protecting Critical Infrastructure"
July 27, 2021
Testimony of U.S. Department of Transportation Deputy Secretary Polly Trottenberg

Chair Cantwell, Ranking Member Wicker, and Members of the Committee, thank you for the opportunity to testify before you today, and for your support of the Department of Transportation (DOT). I am honored to be here with TSA Administrator Pekoske to discuss the security of our nation's pipeline system.

The nexus between transportation infrastructure and national security centers on global competitiveness, climate change, and cybersecurity. As a nation, we need to take all three seriously. Today we will focus on the cybersecurity of a critical component of our national infrastructure: the pipelines that help to fuel and power our homes, our businesses, and our cars, trucks, and airplanes.

I. *Cybersecurity Risks that Threaten Transportation Safety*

In recent years, advances in hardware, software, and computational capabilities have brought significant safety and efficiency benefits to our pipeline system. However, these advances, along with the merging of digital and physical systems and the increased reliance on data, are

introducing new cybersecurity risks to the integrity and availability of pipeline operations. We face persistent and increasingly sophisticated cyber attacks. And the Colonial Pipeline ransomware attack starkly demonstrated how serious the consequences could be for a key part of our national economy and all the Americans who rely on it. These risks require proactive, coordinated, and agile responses.

Today, I will speak with you about DOT's role in pipeline and transportation cybersecurity; our collaboration with the Department of Homeland Security's (DHS's) Transportation Security Administration (TSA) and Cybersecurity and Infrastructure Security Agency (CISA), Department of Energy, which was the designated lead for the Colonial response, other agencies, and the private sector; and the lessons learned from our response to the Colonial attack.

II. *DOT's Role and Modal Authorities*

Depending on the mode of transportation, the level of public versus private ownership, and the authorities of our interagency partners, the Department of Transportation has different levels of authorities and responsibilities over cybersecurity.

DOT's Pipeline and Hazardous Materials Safety Administration (or "PHMSA") oversees pipeline safety. PHMSA protects the American

people and the environment with the safe operation of nearly 3 million miles of pipelines, 17,000 underground storage tanks, and more than 160 Liquefied Natural Gas facilities, as well as the safe packaging and 1.2 million daily shipments of hazardous materials. Pipelines, the vast majority of which fall under private ownership, are a critical component of our energy transportation infrastructure and quite literally power the U.S. economy.

PHMSA has over 550 employees and a budget of $288M. With respect to cybersecurity, PHMSA is pursuing the means to leverage its authorities to inspect and enforce three critical components of pipeline operations:

- Pipeline control room regulations, which are the "nerve centers" of pipeline system operations;
- Integrity management plan requirements; and
- Emergency response plan regulations.

Through these authorities, PHMSA regulates–and will regulate—at the nexus between safe pipeline operations and cybersecurity. We coordinate closely with DHS in the regulation of pipelines, particularly through the relationship between the Transportation Security Administration and PHMSA. A Memorandum of Understanding

recently updated as directed by Congress in the TSA Modernization Act of 2018 delineates the roles and responsibilities of PHMSA and TSA regarding the regulation of pipelines. The MOU promotes communications, efficiency, and a non-duplication of efforts between PHMSA and TSA.

More broadly, many offices across DOT work together to manage cybersecurity risks across our transportation system. Our Office of Intelligence, Security, and Emergency Response engages with the National Security Council and interagency partners on a natural gas pipelines Industrial Control Systems Cybersecurity Initiative and other work to tackle cyber threats from adversaries who seek to compromise critical systems that are essential to U.S. national and economic security.

Our Policy office coordinates cybersecurity policy implementation across our nine Operating Administrations. Our Research and Technology office and Volpe National Transportation Systems Center support our Operating Administrations to conduct research on cybersecurity solutions and best practices as well as gaps that require new approaches.

Finally, the Department's Office of the Chief Information Officer (OCIO) manages internal cybersecurity initiatives and has led our

agency's response to the Executive Order on Improving the Nation's Cybersecurity (EO 14028). In support of this Executive Order, the OCIO is recruiting for new cybersecurity talent, has begun deploying new capabilities, initiated a data sensitivity review, and has developed new proposals to encrypt and protect data. The OCIO is also collaborating with DOT Human Resources on management of DOT's cybersecurity workforce.

Through all these efforts, DOT continues work with our sister agencies, especially TSA and CISA, to invest in world class research and pursue initiatives to address cybersecurity threats, including risks to future transportation technologies and innovations.

III. DOT's Collaboration with Federal and Private Sector Partners

When it comes to pipeline cybersecurity, coordination, and collaboration among our Federal partners is critical. Although DOT and TSA are the co-sector risk management agencies for transportation safety and security—including pipelines, CISA is the lead on cybersecurity risk across critical infrastructure. CISA provides alerts, warnings, advisories, guidance, and resources to help critical infrastructure owners and operators bolster their cyber defenses.

DOT amplifies CISA's outreach by further distributing their vital messages to sector stakeholders. DOT and DHS also encourage the stakeholders to adopt the voluntary National Institute of Standards and Technology Cybersecurity Framework, created through collaboration between industry and government.

Protecting against malicious cyber actors requires the Federal Government to partner with the private sector, which owns, operates, and manufactures most of America's pipeline systems. The private sector has a responsibility to adapt to the continuously evolving cyber threat environment, to build and operate products securely, and protect the security of critical infrastructure in partnership with the Federal Government.

IV. Colonial Pipeline Successful Response and Lessons Learned

When the Colonial Pipeline cybersecurity hack occurred on May 7, 2021, President Biden immediately directed a whole of government approach to respond to the attack. Under the leadership of Secretary Buttigieg, DOT acted quickly to facilitate the transport of fuel to affected regions, and to help get the pipeline system back up and running.

PHMSA engaged around the clock, monitored the safety of the pipeline, and worked with the pipeline company to help ensure a safe restart. With our support, within days, the Pipeline was able to move nearly a million barrels of fuel on a manual basis.

Traditionally, PHMSA regulates safe pipeline operations, and TSA regulates cybersecurity. However, as we saw with the Colonial Pipeline, cybersecurity can and does affect safe and reliable operations. In the wake of this incident, PHMSA is revisiting the scope of integrity management plan and emergency response plan requirements—to ensure they account for cybersecurity attack contingencies.

PHMSA also continues to work closely with DHS and Federal partners, and shares information we receive through our inspection processes.

V. Conclusion

The Colonial Pipeline cybersecurity incident spotlighted the importance of trusted and timely information sharing as well as public and private sector partnership in transportation cybersecurity. It also underscored that we need to keep learning and adapting quickly to meet increasingly complex and sophisticated cybersecurity challenges. DOT will continue to work across the Federal Government and with the private sector to

advance the cybersecurity of the pipelines that fuel and sustain our nation.

Our transportation infrastructure has long been a bedrock of our national security and economic prosperity. At DOT, we look forward to working with this Committee and our agency and White House partners to strengthen and protect that infrastructure. Thank you again for the opportunity to testify, and I will be happy to answer your questions.