TESTIMONY
OF
PATRICIA F.S. COGSWELL
SENIOR STRATEGIC ADVISOR FOR NATIONAL SECURITY
GUIDEHOUSE

For the

UNITED STATES HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

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

October 26, 2021

Chairman Thompson, Ranking Member Katko, and distinguished members of the Subcommittees, thank you for the opportunity to testify before you this morning on Transportation Cybersecurity.

The insights I will share with the Committee today are informed by my 24 years of federal service, my longstanding tenure as a founding member of DHS serving on Day 1, and the varied capacities in which I have served the transportation security mission of DHS through my retirement as Deputy Administrator for the Transportation Security Administration.
My first significant engagement in countering cybersecurity threats to industrial control systems (ICS) was while I served as Special Assistant to the President for Transborder Security, at the National Security Council after the 2012 cyberattack on Saudi Aramco.

Since that time, I've seen:

- The number of cyber *threats* increase – with an expanding number and type of threat actors, including both state and non-state actors, including transnational criminal entities;
- Targeted exploitation of *vulnerabilities* in ICS-environment management practices;
- An increased recognition of the *risk* faced across our critical transportation infrastructure, from the combination of threat, vulnerability, and consequence; and
- Partnership across government and industry to develop tools, programs, information sharing mechanisms, and standards to *mitigate* the risk, including the NIST Framework for *Improving Critical Infrastructure Security*, TSA's Pipeline Security *Guidelines*, and various multi-entity exercises, such as 2020 Ohio Cyber shield.

I am pleased to be here today to speak before the Committee, and hope that I can assist you as you consider how Congress can best support and enable critical infrastructure cybersecurity. I thank you for your willingness to call attention to this very important topic. I also want to

recognize the legislation this Committee, along with Senate Homeland Security and Government Affairs, and the Defense Armed Services Committee are leading to promote and standardize cyber incident reporting to DHS' Cybersecurity and Critical Infrastructure Agency (CISA).

As this Committee further examines how to incentivize the right mix of roles, responsibilities, and activities across government and industry, I'd highlight the following areas as important in our common interest in making progress:

- The value of TSA's authority to issue Security Directives. SDs have repeatedly demonstrated their value, providing a mechanism for TSA and industry, often in concert with DOT and other federal entities, to put immediate measures into place – and sending a clear message to our adversaries, to the American people, and to our allies. After the recent pipeline ransomware event, there was an understandable interest across the Administration, Congress, industry, and the public in taking action. TSA's authority to issue Security Directives for the transportation industry in response to emerging threats was the tool of choice to rapidly direct owners and operators of pipeline and natural gas facilities to implement necessary cyber protections. TSA's SDs are most effective when TSA and the regulated industries work together throughout the process to ensure that requirements are achievable under the timelines set and the regulated industries, all the way down the individual companies can work through implementation.

- Promote bi-directional partnership through analysis of reporting data. As I've spoken with individuals in industry and government about the new CISA cyber security reporting requirements, several colleagues expressed their interest in using this to promote a deeper understanding and engagement of cyber threats to critical infrastructure, particularly where they can be done in a classified setting. While there are significant differences in transportation modes of operation, there is a recognition that analyzing the threats and vulnerabilities associated with industrial control systems across critical infrastructure sectors can tell us more about the prevalence and use of adversaries' tactics, the effectiveness of measures to counter those tactics, and best practices to follow. That analysis is also critical to feed back to the industries required to report cyber incidents to provide them with that deeper understanding of the threats and vulnerabilities to proactively assess additional areas of focus for their own systems and operations. These should then be considered for adoption and reinforcement through regulatory programs.

- Invest in continued evolution of open standards. NIST and DHS, through both CISA and TSA, along with other agencies, have established a cyber standards environment for ICS and critical infrastructure. This environment provides transportation owners and operators with insight and visibility, as well as the opportunity to participate in standards development. It also creates a mechanism to communicate direction to solutions developers and providers.

- Incentivize and encourage innovative approaches, while requiring transportation operators to achieve minimum standards. Consistent with our approach to other transportation security issues, DHS should look to advance regulatory requirements for transportation operators. These could be a formalization of actions already encouraged now or recognized industry best practices, such as the validated architecture reviews, with the aim of changing over time

as the standards evolve. By setting these baseline requirements, we can ensure that critical infrastructure operators are on an even playing field, and that the industry as a whole is less vulnerable to the actions of a small few.

The government should also consider innovative mechanisms for how to achieve these goals, using a model that emphasizes performance-based outcomes, and allows industry to use alternative methods to reach compliance. A more open model also addresses the issues associated with vendor lock or over reliance on a single set of tools, which can disincentivize innovation. Cybersecurity, it's often said, is a team sport. Having as many players on the field with standards based solutions interoperable solutions will enable innovation and enhance the protection of our critical infrastructure.

I would also encourage DHS to establish a regulatory environment where a transportation operator can use a qualified third party entity to complete the cybersecurity architecture reviews or planning required. From a statutory and regulatory perspective, this could look similar to how TSA established the third party canine program. This type of model would increase speed of adoption, and provide transportation operators options for meeting the requirements. But, from industry colleagues I have talked to, transportation operators must have access to a list of government approved third party entities, or be able to rely on firms that meet specified criteria. My understanding is that the pipeline industry is already working to begin to identify those criteria and identifying firms who could serve these needs. To scale this model effectively given the number of critical infrastructure entities, both public and private, that would benefit from industrial control systems cybersecurity expertise, it may make sense to look to GSA to manage the vendor qualification process, with DHS and other entities contributing their expertise, similar to other cross-cutting needs.

As you consider statutory language, I would encourage you to develop it in a way that will create an enduring framework that supports the evolution of cybersecurity as the threats and risks continue to change. A technology neutral approach based on open standards that promote competition, innovation and interoperability should be the core of any such effort.

Thank you again for the opportunity to testify before you today. I look forward to your questions.