CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

Statement before the

House Homeland Security Cybersecurity, Infrastructure Protection & Innovation Subcommittee and Transportation & Maritime Security Subcommittee

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

A Testimony by:

Suzanne Spaulding

Senior Advisor, Center for Strategic and International Studies, and former Under Secretary for the National Protection and Programs Directorate, Department of Homeland Security

Tuesday, October 26, 2021

Virtual

Chairwoman Clarke, Chairwoman Watson Coleman, Ranking Member Garbarino, Ranking Member Gimenez, and distinguished Members of the Subcommittees, thank you for this opportunity to testify today in this joint hearing on the important issue of ensuring the security and resilience of the aviation, rail, and pipeline sectors against significant disruption from malicious cyber activity.

The safety and security of these three sectors falls under the Transportation Security Administration (TSA) at the Department of Homeland Security (DHS). This Spring, following a ransomware incident at Colonial Pipeline that disrupted fuel deliveries along the East Coast and led to panic buying, long lines, and higher prices at gas stations, TSA issued a security directive mandating that certain pipeline owner/operators – those deemed by TSA to be most critical – assess whether their current operations are consistent with TSA's Guidelines on cybersecurity, identify any gaps and remediation measures, and report the results to TSA and others. This was followed in July 2021 with an additional cybersecurity directive mandating implementation of cybersecurity mitigation measures; development of Cybersecurity Contingency Response Plans in the event of an incident; and an annual cybersecurity architecture design review, among other things.

Recently, the Secretary of Homeland Security announced that DHS would be coming out with similar mandates covering critical U.S. airport operators, passenger aircraft operators, and all cargo aircraft operators, as well as "higher-risk" railroad and rail transit assets.[1]

The pipeline directives have not been publicly released and the aviation and rail directives are still under development. However, they have generally been described as prescribing a relatively basic level of cybersecurity measures and plans for incident response. The latter, planning and exercising incident response to reduce the impact of a successful hack is one of the most important, and often underappreciated, elements of managing cyber risk.

The details will be important but, as described, these directives seem like a step in the right direction. Moving forward, TSA will need to operate collaboratively with these sectors to ensure that the requirements and timelines drive toward actual improvements in security and resilience. No directives or regulations will achieve perfect security. This is an exercise in risk management, not risk elimination, which is why planning for incident response is so crucial. The objective should be to ensure that the relevant industries are putting in place a common baseline of measures to strengthen the security and resilience of the highest-risk assets.

As the former Under Secretary at the Department of Homeland Security leading what is now called the Cybersecurity and Infrastructure Security Agency (CISA), as a member of the Congressionally-created Cyberspace Solarium Commission (CSC), and going back to my

[1] https://thehill.com/policy/cybersecurity/575580-tsa-to-issue-regulations-to-secure-rail-aviation-groups-against-cyber?rl=1

involvement with the Commission on Cybersecurity for the 44th President, which was run out of my current organization, the Center for Strategic and International Studies (CSIS), I have always favored voluntary, market-based solutions to cybersecurity. Markets are generally more efficient and, important for such a dynamic area as cyber, nimbler. However, over the last couple of years, I have reluctantly had to conclude that we cannot rely upon markets alone to ensure the continuity of nationally critical functions upon which the American public relies. I think there are several reasons for this.

The first is that the purely voluntary approach has not gotten us where we need to be, despite decades of effort. There has been significant progress and a growing level of maturity in industry and in government on cyber, including in the sectors under discussion today. All three, aviation, rail, and pipelines, have worked collaboratively with DHS over the years to improve their physical and cyber security. But the threat is evolving much more quickly than our defense. There is an urgency to addressing this risk to the American public that the market simply cannot address fast enough.

One reason the market has not fully addressed this challenge is the paucity of information. Markets need information to function effectively. For example, information about the scale, scope, and cost of inadequate cybersecurity is needed to drive a demand signal that would prompt appropriate levels of investment and balance the "first-to-market" imperative. Yet, since most cyber incidents are not reported, and those that are do not provide details on costs, this information is lacking. Furthermore, such information is needed to calculate the return on investment (ROI) for security measures. Without it, security professionals often have a hard time convincing management to make needed investments.

Even in a perfect market, there are external impacts on society and the nation from inadequate cybersecurity, particularly in assets that control essential functions, that will not be captured in a businesses' bottom line or ROI. Externalities have long justified regulation and mandates, such as with pollution and highway safety. In the case of pipelines, rail, and aviation, the potential risks to public health and safety, as well as the potential for cascading economic consequences, calls for a government role.

This is the thinking behind a number of the recommendations from the Cyberspace Solarium Commission. First, we looked at ways to improve the performance of relevant markets, including by providing better market incentives to improve the cybersecurity behavior of firms. Mandatory reporting of relevant cyber incidents can fill critical information gaps, particularly if paired with the establishment of a Bureau of Cyber Statistics. Bolstering the capabilities of cyber insurance underwriters can help that industry play the role it does in other risk categories to encourage appropriate investments in security and safety.

In addition to nudging firms in the sector toward better cybersecurity behavior, the Federal government can do more to help these firms make better purchasing decisions regarding the security of the products and services they deploy as part of their business. More government-sponsored security testing of critical technologies and applications—like industrial control systems—can help firms understand the security characteristics of the devices they deploy. The CSC recommended the creation of government-sponsored critical technology security centers at places like federally-funded research and development centers or national labs to fill this gap. Similarly, a clearer ecosystem of cybersecurity product certifications would allow procurement specialists at critical firms in the sector to more easily price security into their purchasing decisions and manage their supply chain risk.

But the CSC, too, ultimately concluded that the market was not going to be sufficient to provide the level of security and resilience that is urgently needed for the most important elements of our infrastructure, particularly what CSC calls Systemically Important Critical Infrastructure. The Solarium recommended creating a robust and transparent methodology for identifying these most critical systems and assets and then building a closer relationship between SICI firms and the Federal government through a suite of benefits—like improved intelligence sharing and operational support— but also burdens—like requirements for security behavior and enhanced incident reporting.

Consistent with this thinking, I believe it is appropriate for TSA to use its existing authority to put basic requirements in place for the most critical assets in these three sectors. That said, the process is important. According to testimony from Kimberly Denbow Managing Director, Security & Operations American Gas Association, in front of this committee in September in support of the legislation to mandate cyber incident reporting across critical infrastructure, "The TSA Pipeline Group has been the epitome of innovation – leveraging the infrastructure subject matter expertise of pipeline operators, partnering with CISA and Idaho National Labs for in-house industrial control system cybersecurity knowledge, and collaborating with the Department of Transportation's Pipeline and Hazardous Materials Safety Administration (PHMSA) on cybersecurity reviews of control centers. AGA helped champion the CISA/TSA Pipeline Cybersecurity Initiative and promoted effortlessly the Pipeline Validated Architectural Design Reviews. The quality output has been the result of the dedication of TSA and CISA staff, in partnership with pipeline operators, towards a shared common goal – pipeline security."[2]

This level of collaboration should be the model as TSA, in partnership with CISA, works to develop the aviation and rail directives. Industry has a level of expertise that will be essential in understanding what needs to be done. Businesses rarely embrace government mandates; that is not surprising. Nevertheless, industry must be at the table to help craft directives that are ambitious

[2] https://homeland.house.gov/imo/media/doc/2021-09-01-CIPI-HRG-Testimony-Denbow.pdf

but achievable, and government must invite them early enough in the process to allow to make a meaningful contribution.

It’s also important to note that the security directive process allows the TSA Administrator flexibility to work with businesses even after the directive is issued. For example, a company can propose alternative measures for achieving the objective(s), and the Administrator can amend or issue new directives as conditions warrant.

DHS has indicated that these temporary directives will be replaced with regulations, presumably no later than one year from their issuance, when they are set to expire. The informal consultation with industry will, pursuant to the Administrative Procedures Act, be supplemented by a formal notice and comment process. Not only should the industries directly covered by the proposed regulations weigh in, those who depend upon these critical sectors should also let their voices be heard as the government considers how best to ensure the security, safety, and reliability of these critical functions in the face of growing cyber risks. In addition, these regulations should be informed by an awareness of the tools and technologies that are available to help these asset owners and operators gain visibility into their information technology (IT) and operational technology (OT) systems, detect malicious activity, and respond quickly and effectively. To encourage continued innovation in this area, government should lean towards open, performance-based standards that are technology neutral and vendor agnostic.

Furthermore, any new regulations should draw on existing guidelines, standards, and best practices. They should be harmonized with requirements in other sectors, particularly as between the pipeline and electric sectors, in which there is often significant overlap.

Finally, TSA has been working to build its cyber capacity, but it should not try to duplicate expertise that resides at CISA. These two DHS entities should continue to work closely together, with TSA bringing industry relationships and expertise together with CISA’s cyber-specific and critical infrastructure resilience expertise. The work of the National Risk Management Center should inform the identification of highest-risk/highest-consequence functions. Congress needs to ensure that DHS is provided the resources necessary to effectively implement these mandates and to continue its equally important voluntary work with these vital industries.

Time is not on our side. The threat environment grows more dangerous with each passing day. In the recent words of one Administration official, “the overall environment is more aggressive; more sophisticated; and more belligerent...”[3]

[3] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr

The general assessment is that neither state nor non-state actors have current intent to cause significant disruption. But cyber incidents can have unintended consequences. NotPetya came back to impact Russian companies. And if we are to believe the criminals involved in the Colonial Pipeline attack, they did not intend to disrupt pipeline operations. I am inclined to believe that, since it would've been hard to predict that an intrusion into the corporate IT system, as opposed to the OT system, would have such a significant impact on operations. It is a reminder that lack of intent should not give us great comfort.

Moreover, intent can change. Even short of a direct kinetic conflict in which an adversary might decide to disrupt our critical infrastructure, there is the prospect of an adversary using the credible threat of such disruption to deter us from taking actions in our national interest. Having this leverage could embolden China in the South China Sea or Russia in Ukraine or elsewhere, for example. It seems likely that Russia's cyber attacks on Ukraine's electric grid were designed not only to undermine the Ukraine government but to send a signal to the U.S. about Russia's capabilities.

Perhaps most troubling is the threat of a destructive attack on the safety systems of operations, leading not just to disruption but to potentially catastrophic deadly consequences. In 2017, a Saudi petrochemical plant was hit with malware later dubbed "Triton" which disabled the Safety Instrumented System (SIS). SISs are the last line of automated safety defense for industrial facilities, designed to prevent equipment failure and catastrophic incidents such as explosions or fire. Faulty code prevented that attack from succeeding but experts say the technique is replicable by others. Moreover, in 2019, the attackers behind the Triton malware, attributed to a Russian government-funded research institution, were reported to be scanning and probing at least 20 electric utilities in the United States for vulnerabilities.

The bipartisan co-chairs of the Solarium have noted that it was envisioned as a 9/11 commission to avert a cyber 9/11. We should not wait for a tragedy caused by malicious cyber activity in one of these vital sectors before we take the necessary action. The proposed TSA directives reflect a growing body of evidence that the risk of serious disruptions to critical infrastructure is not "potential" or in the future, it is here now and requires an urgent response.

Thank you and I look forward to your questions.