IMPACTS OF EMERGENCY AUTHORITY CYBERSECURITY REGULATIONS ON THE TRANSPORTATION SECTOR

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

NOVEMBER 19, 2024

Serial No. 118–82

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
60–114 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

Mark E. Green, MD, Tennessee, *Chairman*

Michael T. McCaul, Texas
Clay Higgins, Louisiana
Michael Guest, Mississippi
Dan Bishop, North Carolina
Carlos A. Gimenez, Florida
August Pfluger, Texas
Andrew R. Garbarino, New York
Marjorie Taylor Greene, Georgia
Tony Gonzales, Texas
Nick LaLota, New York
Mike Ezell, Mississippi
Anthony D'Esposito, New York
Laurel M. Lee, Florida
Morgan Luttrell, Texas
Dale W. Strong, Alabama
Josh Brecheen, Oklahoma
Elijah Crane, Arizona

Bennie G. Thompson, Mississippi, *Ranking Member*
Eric Swalwell, California
J. Luis Correa, California
Troy A. Carter, Louisiana
Shri Thanedar, Michigan
Seth Magaziner, Rhode Island
Glenn Ivey, Maryland
Daniel S. Goldman, New York
Robert Garcia, California
Delia C. Ramirez, Illinois
Robert Menendez, New Jersey
Thomas R. Suozzi, New York
Timothy M. Kennedy, New York
LaMonica McIver, New Jersey
Yvette D. Clarke, New York

Stephen Siao, *Staff Director*
Hope Goins, *Minority Staff Director*
Sean Corcoran, *Chief Clerk*

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

Carlos A. Gimenez, Florida, *Chairman*

Clay Higgins, Louisiana
Nick LaLota, New York
Laurel M. Lee, Florida
Mark E. Green, MD, Tennessee *(ex officio)*

Shri Thanedar, Michigan, *Ranking Member*
Robert Garcia, California
Timothy M. Kennedy, New York
Bennie G. Thompson, Mississippi *(ex officio)*

Vacancy, *Subcommittee Staff Director*
Alex Marston, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

The Honorable Carlos A. Gimenez, a Representative in Congress From the State of Florida, and Chairman, Subcommittee on Transportation and Maritime Security:

Oral Statement 1

Prepared Statement 3

The Honorable Shri Thanedar, a Representative in Congress From the State of Michigan, and Ranking Member, Subcommittee on Transportation and Maritime Security:

Oral Statement 4

Prepared Statement 5

The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:

Prepared Statement 6

WITNESSES

Panel I

Mr. Steve Lorincz, Deputy Executive Assistant Administrator, Security Operations, Transportation Security Administration, U.S. Department of Homeland Security:

Oral Statement 7

Joint Prepared Statement 8

Mr. Chad Gorman, Deputy Executive Assistant Administrator, Operations Support, Transportation Security Administration, U.S. Department of Homeland Security:

Oral Statement 12

Joint Prepared Statement 8

Ms. Tina Won Sherman, PhD, Director, Homeland Security and Justice, U.S. Government Accountability Office:

Oral Statement 14

Prepared Statement 15

Panel II

Mr. Ian Jefferies, President & Chief Executive Officer, Association of American Railroads:

Oral Statement 33

Prepared Statement 35

Ms. Kimberly Denbow, Vice President, Security Operations, American Gas Association:

Oral Statement 37

Prepared Statement 39

FOR THE RECORD

The Honorable Clay Higgins, a Representative in Congress From the State of Louisiana:

Article, November 18, 2024, *The Record*, Recorded Future News 30

Page

APPENDIX

The Honorable Carlos A. Gimenez, a Representative in Congress From the State of Florida, and Chairman, Subcommittee on Transportation and Maritime Security:
Statement of Airlines For America 49

IMPACTS OF EMERGENCY AUTHORITY CYBERSECURITY REGULATIONS ON THE TRANSPORTATION SECTOR

Tuesday, November 19, 2024

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Transportation and
Maritime Security,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room 310, Cannon House Office Building, Hon. Carlos A. Gimenez (Chairman of the subcommittee) presiding.

Present: Representatives Gimenez, Higgins, Lee, and Thanedar.

Mr. Gimenez. Good morning. The Committee on Homeland Security Subcommittee on Transportation and Maritime Security will come to order.

Without objection, the Chair may declare the subcommittee in recess at any point. Today's hearing will examine the Transportation Security Administration's use of security directives and proposed rule making in transportation sector cybersecurity regulations.

I now recognize myself for an opening statement.

Today, the subcommittee is examining how the Transportation Security Administration utilizes security directives and public rules to manage cybersecurity risks within the transportation sector.

In today's interconnected world, cybersecurity is more than just an IT issue. It is a critical component of our national security.

Cyber threats have become pervasive, and their potential impact on critical infrastructure has profound implications for the safety and stability of our society and the resilience of our economy.

Nowhere is this more evident than our transportation systems, which serve as the backbone of the American economy. These systems connect our communities, support commerce, and facilitate the movement of goods and services across the country and around the world.

Our transportation networks, spanning aviation, rail, public transit, highways, pipelines, and maritime ports, are increasingly reliant on complex digital systems for operations and coordination.

This reliance makes them especially vulnerable to cyber attacks by criminal groups and nation-state actors.

Moreover, as emerging technologies like autonomous vehicles, connected infrastructure, and artificial intelligence become more integrated into our transportation system, the cybersecurity threat landscape grows more complex.

These advances, while offering new efficiencies and capabilities, also create additional access points that cyber criminals and nation-state adversaries could exploit.

A cyber attack on any of these systems could disrupt travel, halt commerce, threaten public safety, and create cascading effects across our economy and national security landscape.

Whether through ransomware attacks, data breaches, or other malicious cyber activities, such threats have the potential to cause extensive harm, demonstrating the need for targeted cybersecurity regulations within the transportation sector.

Safeguarding our transportation infrastructure is not only about securing physical assets, it's also about protecting the digital networks that power and control them, ensuring resilience in the face of evolving threats.

The Transportation Security Administration, TSA, established to protect our Nation's transportation systems, has an essential and increasingly complex role in defending these critical networks against cyber threats.

With this mandate to secure the Nation's vast transportation infrastructure, covering everything from aviation and rail to maritime and public transit, TSA is tasked not only with physical security, but also with developing and enforcing cybersecurity regulations across the industry.

I have concerns about TSA's current approach. In recent years, TSA has issued numerous security directives aimed at addressing cyber risks.

However, these directives often seem reactive, hastily implemented, and lacking the necessary consultation with stakeholders.

Industry feedback indicates that these directives can be overt, overly prescriptive rather than performance-based, limiting operators' abilities to tailor cybersecurity practices to their specific operational needs.

A security directive that lacks clarity and flexibility may do more harm than good. Instead of fostering robust security measures, it can lead to confusion in efficiency and check-box mentality, where compliance is valued over actual risk reduction.

Moreover, the lack of collaboration with industry experts, the people who understand these systems best, raises concerns about whether these directives are even capable of addressing the most pressing vulnerabilities.

On November 6, less than 2 weeks ago, TSA issued a Notice of Proposed Rulemaking that aimed to establish mandatory cyber risk management and reporting requirements for certain surface transportation owners and operators.

The sheer complexity of these regulations, spanning over 300 pages, is overwhelming, especially considering smaller operators who are already operating with limited resources.

These proposed rules raise an important question: Will they effectively fulfill their intended purpose by reducing cybersecurity risk within the transportation sector, or will they simply place an undue burden on operators?

TSA should empower operators with the flexibility to develop and implement tailored cybersecurity strategies that best address their unique risks and operational needs.

When I was the mayor of Miami-Dade County, I focused on reducing overhead and streamlining regulations to enable business innovation and improve government efficiency.

I believe the same approach is essential as we work to effectively protect our Nation's transportation systems from cybersecurity risks. By balancing regulatory standards with operational adaptability, we can promote robust cybersecurity practices that both protect critical infrastructure and foster innovation and efficiency within the industry.

Thank you to our witnesses from both panels for appearing before the subcommittee. I look forward to your testimony.

[The statement of Chairman Gimenez follows:]

Statement of Chairman Carlos A. Gimenez

Today, this subcommittee is examining how the Transportation Security Administration utilizes Security Directives and Public Rules to manage cybersecurity risks within the transportation sector.

In today's interconnected world, cybersecurity is more than just an IT issue—it's a critical component of our national security.

Cyber threats have become pervasive, and their potential impact on critical infrastructure has profound implications for the safety and stability of our society and the resilience of our economy.

Nowhere is this more evident than in our transportation systems, which serve as the backbone of the American economy. These systems connect our communities, support commerce, and facilitate the movement of goods and services across the country and around the world.

Our transportation networks, spanning aviation, rail, public transit, highways, pipelines, and maritime ports, are increasingly reliant on complex digital systems for operation and coordination. This reliance makes them especially vulnerable to cyber attacks by criminal groups and nation-state actors.

Moreover, as emerging technologies like autonomous vehicles, connected infrastructure, and artificial intelligence become more integrated into our transportation systems, the cybersecurity landscape grows more complex.

These advances, while offering new efficiencies and capabilities, also create additional access points that cyber criminals and nation-state adversaries could exploit.

A cyber attack on any of these systems could disrupt travel, halt commerce, threaten public safety, and create cascading effects across our economy and national security landscape.

Whether through ransomware attacks, data breaches, or other malicious cyber activities, such threats have the potential to cause extensive harm, demonstrating the urgent need for targeted cybersecurity regulations within the transportation sector.

Safeguarding our transportation infrastructure is not only about securing physical assets—it is also about protecting the digital networks that power and control them, ensuring resilience in the face of evolving threats.

The Transportation Security Administration (TSA), established to protect our Nation's transportation systems, has an essential and increasingly complex role in defending these critical networks against cyber threats.

With its mandate to secure the Nation's vast transportation infrastructure—covering everything from aviation and rail to maritime and public transit—TSA is tasked not only with physical security, but also with developing and enforcing cybersecurity regulations across the industry.

I have concerns about the TSA's current approach. In recent years, TSA has issued numerous Security Directives aimed at addressing cyber risks. However, these directives often seem reactive, hastily implemented, and lacking the necessary consultation with stakeholders.

Industry feedback indicates that these directives can be overly prescriptive rather than performance-based, limiting operators' ability to tailor cybersecurity practices to their specific operational needs.

A Security Directive that lacks clarity and flexibility may do more harm than good. Instead of fostering robust security measures, it can lead to confusion, inefficiency, and a checkbox mentality, where compliance is valued over actual risk reduction.

Moreover, the lack of collaboration with industry experts—the people who understand these systems best—raises concerns about whether these directives are even capable of addressing the most pressing vulnerabilities.

On November 6, less than 2 weeks ago, TSA issued a Notice of Proposed Rulemaking that aims to establish mandatory cyber risk management and reporting requirements for certain surface transportation owners and operators.

The sheer complexity of these regulations—spanning over 300 pages—is overwhelming, especially considering smaller operators who are already operating with limited resources.

These proposed rules raise an important question: will they effectively fulfill their intended purpose by reducing cybersecurity risks within the transportation sector, or will they simply place an undue burden on operators?

TSA should empower operators with the flexibility to develop and implement tailored cybersecurity strategies that best address their unique risks and operational needs.

When I was mayor of Miami-Dade County, I focused on reducing overhead and streamlining regulations to enable business innovation and improve government efficiency. I believe this same approach is essential as we work to effectively protect our Nation's transportation systems from cybersecurity risks.

By balancing regulatory standards with operational adaptability, we can promote robust cybersecurity practices that both protect critical infrastructure and foster innovation and efficiency within the industry.

Thank you to our witnesses from both panels for appearing before the subcommittee.

I look forward to your testimony.

Mr. GIMENEZ. I now recognize the Ranking Member, the gentleman from Michigan, Mr. Thanedar, for his opening statements.

Mr. THANEDAR. Good morning, everyone. Thank you, Chairman Gimenez, for holding today's hearing, and thank you to our witnesses for joining us.

The May 2021 ransomware attack against Colonial Pipeline served as a major turning point in TSA's approach to securing transportation systems from cyber attacks.

Prior to the attack, TSA's efforts to ensure the cybersecurity of transportation systems relied largely upon voluntary cooperation and adoption of recommended guidelines and best practices.

The attack had far-reaching impacts as Colonial Pipeline shut down the transportation of fuel throughout the pipeline, which services much of Southeastern United States. The public flocked to gas stations, leading to long lines and fuel shortages.

In the aftermath of the attack, TSA assumed a more regulatory posture toward transportation cybersecurity, acting quickly to issue the first ever cybersecurity directives for pipeline systems and facilities.

TSA followed that initial security directive with similar mandates for owners and operators of freight rail, passenger rail, public transit systems, as well as changes to security programs for airports and air carriers.

TSA required owners and operators to adopt essential cybersecurity measures, such as designating a cybersecurity coordinator and reporting cyber incidents.

TSA engaged extensively with industry stakeholders and quickly learned that its mandate were viewed as too prescriptive and inflexible.

To provide regulated parties with enough flexibility to innovate and respond to evolving threats, TSA developed a novel approach in subsequent directives, focusing on desired performance and security outcomes rather than specific measures.

Over the past couple years, TSA has continued to refine its approach through extensive engagement with stakeholders. Earlier this month, TSA issued a Notice of Proposed Rulemaking to clarify cybersecurity requirements for owners and operators of pipeline rails and over-the-road bus systems.

TSA's proposal, which is currently open for comments, would require system owners and operators to establish and execute a comprehensive cyber risk management program, representing a significant step forward in the evolution of TSA's cybersecurity efforts.

The maturation of those efforts is also reflected in recent adjustments to TSA's investment in cybersecurity.

In fiscal year 2021, prior to the Colonial Pipeline attack, Congress funded TSA cybersecurity activities at $86 million with 86 dedicated positions.

Now, in fiscal year 2024, that investment has increased to $137 million and 167 positions.

For fiscal year 2025, the Biden-Harris administration has requested an additional increase of $8 million and 41 positions.

I hope Congress will continue to support TSA's efforts to enhance the cybersecurity of the transportation sector.

To those who may question the need for regulations or TSA's use of emergency security directives, I would note that if TSA continued to rely on voluntary compliance with recommended guidelines and another attack like the attack on Colonial Pipeline were to occur, the public would rail against both TSA and Congress for allowing a disproven approach to continue.

Our adversaries are continuing to adapt and pursue offensive cyber capabilities. Now is the time for TSA and its partners to ensure our security defenses are fully fortified.

I thank the Chairman and our witnesses again, and I yield back.

[The statement of Ranking Member Thanedar follows:]

Statement of Ranking Member Shri Thanedar

November 19, 2024

The May 2021 ransomware attack against Colonial Pipeline served as a major turning point in TSA's approach to securing transportation systems from cyber attacks.

Prior to the attack, TSA's efforts to ensure the cybersecurity of transportation systems relied largely upon voluntary cooperation and adoption of recommended guidelines and best practices.

The attack had far-reaching impacts, as Colonial Pipeline shut down the transportation of fuel through the pipeline, which services much of the Southeastern United States.

The public flocked to gas stations, leading to long lines and fuel shortages.

In the aftermath of the attack, TSA assumed a more regulatory posture toward transportation cybersecurity, acting quickly to issue the first-ever cybersecurity directives for pipeline systems and facilities.

TSA followed that initial security directive with similar mandates for owners and operators of freight rail, passenger rail, and public transit systems, as well as changes to security programs for airports and air carriers.

TSA required owners and operators to adopt essential cybersecurity measures, such as designating a cybersecurity coordinator and reporting cyber incidents.

TSA engaged extensively with industry stakeholders and quickly learned that its mandates were viewed as too prescriptive and inflexible.

To provide regulated parties with enough flexibility to innovate and respond to evolving threats, TSA developed a novel approach in subsequent directives, focusing on desired performance and security outcomes rather than specific measures.

Over the past couple years, TSA has continued to refine its approach through extensive engagement with stakeholders.

Earlier this month, TSA issued a notice of proposed rulemaking to codify cybersecurity requirements for owners and operators of pipeline, rail, and over-the-road bus systems.

TSA's proposal, which is currently open for comment, would require system owners and operators to establish and execute a comprehensive cyber risk management program, representing a significant step forward in the evolution of TSA's cybersecurity efforts.

The maturation of those efforts is also reflected in recent adjustments to TSA's investment in cybersecurity.

In fiscal year 2021, prior to the Colonial Pipeline attack, Congress funded TSA's cybersecurity activities at $86 million, with 86 dedicated positions.

Now, in fiscal year 2024, that investment has increased to $137 million and 167 positions.

For fiscal year 2025, the Biden-Harris administration has requested an additional increase of $8 million and 41 positions.

I hope Congress will continue to support TSA's efforts to enhance the cybersecurity of the transportation sector.

To those who may question the need for regulations or TSA's use of emergency security directives, I would note that, if TSA continued to rely on voluntary compliance with recommended guidelines and another attack like the attack on Colonial Pipeline were to occur, the public would rail against both TSA and Congress for allowing a disproven approach to continue.

Our adversaries are continuing to adapt and pursue offensive cyber capabilities; now is the time for TSA and its partners to ensure our security defenses are fully fortified.

Mr. GIMENEZ. Thank you, Ranking Member Thanedar.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

NOVEMBER 19, 2024

In November 2001, following the September 11 terrorist attacks, Congress passed the Aviation and Transportation Security Act to create the Transportation Security Administration and task the agency with securing all modes of transportation.

Congress provided the TSA administrator broad authority to issue and enforce security measures, including the authority to "issue, rescind, and revise such regulations as are necessary to carry out the functions of the administration."

Congress also recognized that threats to transportation would likely evolve faster than regulatory processes could respond, so Congress provided the TSA administrator with unique authority to bypass the normal rule-making processes and issue regulations or security directives immediately when necessary.

In fact, statute requires that "if the administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

This emergency authority has been essential to TSA's ability to deter, disrupt, and defend against attacks to transportation over the past 23 years.

For example, in August 2006, following the disruption of an al-Qaeda plot to attack transatlantic flights using liquid explosives, TSA used its authority to immediately ban passengers from carrying liquids on flights.

The ban took effect overnight, and TSA issued updated directives in the following days to refine the measures, including to allow limited quantities of liquids.

TSA has similarly issued security directives to respond to intelligence regarding bombs hidden in underwear and personal electronic devices, threats posed by certain powders, plots to hide explosive devices in cargo packages, and public health threats during the COVID–19 pandemic.

When it comes to the cybersecurity of transportation systems, TSA's emergency authorities are arguably even more necessary.

Cyber threats have evolved extremely quickly over the past several years, and the May 2021 ransomware attack against Colonial Pipeline made clear that the voluntary compliance model TSA had previously applied to cybersecurity was insufficient.

In the aftermath of the attack, based on intelligence indicating continued, evolving cyber threats to various modes of transportation, TSA was able to issue security directives that helped protect transportation systems prior to the issuance of a proposed rule making.

TSA's initial cybersecurity requirements were overly stringent and prescriptive—but TSA has worked to refine its approach based on stakeholder feedback.

The same emergency authorities that allowed TSA to take quick action also enabled the agency to fix its mistakes expeditiously.

If TSA had not had the ability to issue security directives immediately, the agency likely would have pursued an overly stringent and prescriptive rule making, leading to an even longer period of disruption, all while transportation systems would have been left vulnerable to attack in the interim.

TSA's cybersecurity efforts have matured significantly over a short time period, resulting in the agency's recent proposed rule making which is focused on security outcomes rather than prescriptive measures.

Though there is still room for further improvement to be achieved through the notice and comment process, the proposed rule making represents a novel, collaborative approach to regulations that should be applauded and encouraged.

Congress should continue to support robust funding for TSA's cybersecurity efforts and promote collaboration between TSA and industry partners—not call into question the critical authorities TSA has leveraged to protect transportation systems.

Mr. GIMENEZ. Again, I am pleased to have a distinguished panel of witnesses before us today on this critical topic. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GIMENEZ. Let the record reflect that the witnesses have answered in the affirmative. Thank you and please be seated.

I would now like to formally introduce our witnesses. Mr. Steve Lorincz serves as the deputy executive assistant administrator for security operations at the Transportation Security Administration.

Mr. Chad Gorman serves as the deputy executive assistant administrator for operations support at the Transportation Security Administration.

Ms. Tina Won Sherman serves as director for the Homeland Security and Justice Team at the Government Accountability Office.

I thank each of our distinguished witnesses for being here today.

I now recognize Mr. Lorincz for 5 minutes to summarize his opening statements.

STATEMENT OF STEVE LORINCZ, DEPUTY EXECUTIVE ASSISTANT ADMINISTRATOR, SECURITY OPERATIONS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. LORINCZ. Good morning, and thank you so much for having me and inviting me for this hearing. My name is Steve Lorincz. As you mentioned, I'm the deputy executive assistant administrator for security operations. I have the privilege to work with and oversee 57,000 employees within security operations.

Under our portfolio, we have domestic aviation operations which oversees 433 airports across the country. We also have international operations which oversees—we have assets throughout the world.

We oversee surface operations, we oversee compliance operations, and we have—we have an administrative function, which oversees their administrative functions within security operations.

We also have 2 senior liaison positions—1 is with CISA, and the other is with the State Department.

So it's a pleasure, once again, to be here. I look forward to the questions, and thank you.

[The joint prepared statement of Mr. Lorincz and Mr. Gorman follows:]

JOINT PREPARED STATEMENT OF CHAD GORMAN AND STEVE LORINCZ

NOVEMBER 19, 2024

Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the committee. My name is Chad Gorman, and I serve as the deputy executive assistant administrator for operations support within the Transportation Security Administration (TSA). I am joined today by deputy executive assistant administrator for security operations, Steve Lorincz. We appreciate the opportunity to appear before you today to discuss TSA's role in cybersecurity for our Nation's transportation infrastructure.

TSA was established by the *Aviation and Transportation Security Act (ATSA),* which was signed into law on November 19, 2001. With the enactment of ATSA, TSA assumed the mission to oversee security in all modes of transportation, be that aviation or the Nation's surface transportation systems—mass transit and passenger rail, freight rail, highway and motor carrier, pipeline, as well as supporting maritime security with our U.S. Coast Guard (USCG) partners. In the years since 9/11, TSA has not only had to address the ever-present physical threats to aviation and surface transportation modes, but also dynamic and emerging cybersecurity threats to our Nation's aviation, rail, highway and motor carrier, hazardous liquid, and natural gas pipeline infrastructure. This is not a mission we can accomplish alone. TSA's mission success is highly dependent on close collaboration and strong relationships with our transportation industry stakeholders and our Federal, State, and local partners, including the Department of Transportation (DOT) as the Department of Homeland Security's (DHS) co-Sector Risk Management Agency for the Transportation System Sector.

TRANSPORTATION CYBERSECURITY THREATS

The August cyber attack at the Seattle-Tacoma International Airport serves as another reminder of the significant disruptions and broader impacts cybersecurity incidents can cause to transportation. Cyber attacks are an evolving and persistent threat. Cyber threat actors, including nation-states, have demonstrated their intent and ability to conduct malicious cyber activity targeting critical infrastructure by exploiting vulnerabilities present in both Operational Technology (OT) (the hardware and software that controls physical devices, processes, and infrastructure) and Information Technology (IT) systems. Unlike traditional kinetic threats we confront, cyber threats are not bound by global borders. They can cross vast distances between our adversaries and U.S.-based critical transportation infrastructure in seconds, drastically impacting our ability to respond successfully with our more traditional and time-bound approaches. Nation-state actors like Russia, China, Iran, and North Korea recognize cyber capabilities bypass geographical limitations and, accordingly, they have developed and demonstrated capabilities that pose significant cyber threats to the United States. The director of national intelligence has stated that our adversaries and strategic competitors possess, and in the case of the People's Republic of China (PRC), have prepositioned cyber attack capabilities that could be used against U.S. critical infrastructure, including transportation, especially during times of increased conflict.

This year, the intelligence community assessed that the PRC almost certainly could launch cyber attacks that could disrupt critical infrastructure within the United States, specifically highlighting oil and gas pipelines and rail systems. In May 2023, the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint Cybersecurity Advisory which highlighted for the first time a cyber threat cluster associated with the PRC identified as Volt Typhoon. There have been subsequent documents released on Volt Typhoon by CISA and other U.S. Government agencies. Volt Typhoon has been active since at least mid-2021 and targets U.S. critical infrastructure entities, including those in the transportation sector. Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence-gathering operations, and the U.S. Government assesses with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks for disruptive or destructive cyber activity against U.S. critical infrastructure in the event of a major crisis or conflict with the United States. Observed behavior suggests Volt Typhoon intends to maintain access without being detected for as long as possible by relying almost exclusively on stealthy "living-off-the-land" techniques in which the cyber threat actor uses legitimate, built-in network administration tools to sustain, advance, and conceal an attack.

In April 2023, after receiving a briefing on the relevant intelligence, the Transportation Security Oversight Board (TSOB) recommended to TSA that a cybersecurity emergency exists that warranted the TSA administrator's determination to expedite the implementation of critical cyber mitigation measures in aviation, which he had done through the exercise of his emergency regulatory authority by issuing Joint Emergency Amendment (EA) 23–01. Joint EA–2301 on March 7, 2023. The Joint EA amended the security programs for covered aviation entities to require performance-based cybersecurity measures intended to prevent the disruption and degradation of their critical systems. Additionally, in April of this year, President Biden extended the national emergency on malicious cyber-enabled activities, citing the continued significant and malicious activities that are posing an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

TSA is dedicated to protecting our Nation's transportation networks against evolving cyber threats and continues to work collaboratively with public and private stakeholders to expand the implementation of intelligence-driven, risk-based policies and programs and continue active information sharing within the Federal Government and with industry to reinforce the security posture of these networks.

ADDRESSING CYBERSECURITY THREATS THROUGH UNIQUE TSA AUTHORITIES

In response to these evolving threats, the TSA administrator has utilized his emergency authorities found in both statute and regulation. In statute, Congress provided the TSA administrator authority to issue regulations and security directives (SDs) immediately to protect transportation security. 49 U.S.C. § 114(l)(2)). In doing so, the administrator may waive certain procedural requirements for traditional notice and comment rule making to carry out TSA's transportation security mission. SDs issued under this authority are subject to review by the Transportation Security Oversight Board (TSOB). The TSOB was established by the Aviation and Transportation Security Act of 2001 (ATSA) and consists of 7 statutorily-prescribed voting members, including DHS, DOT, Department of Justice, Department of Defense, Treasury Department, Office of the Director of National Intelligence, and National Security Council. The Board is chaired by the DHS deputy secretary. The TSOB is charged with reviewing and ratifying, or disapproving, any regulation or SD issued by the TSA administrator under section 114(l)(2) within 30 days after the date of issuance. If a regulation or directive is not ratified by the TSOB, it may remain in effect for no more than 90 days. To date, the TSOB has reviewed and ratified all of TSA's surface cybersecurity SDs. The TSOB also has discretionary authority to review and make recommendations to the administrator regarding transportation security plans. (49 U.S.C. § 115)(c)(5),(6)). Under this authority, the TSOB provided its recommendation to TSA regarding a cybersecurity emergency warranting emergency action in the aviation sector.

By regulation, the TSA administrator has the authority to issue emergency amendments to the security programs of regulated aviation operators. (49 CFR §§ 1542.105, 1544.105, and 1546.105). The administrator may use this authority upon finding that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air commerce. The administrator has additional regulatory authority to issue SDs to regulated aviation operators where it is determined that additional security measures are necessary to respond to a threat assessment or specific threat. (49 CFR §§ 1542.303 and 1544.305.)

The TSA administrator's ability to leverage these authorities and respond immediately during emergency situations has significantly mitigated threats posed by a rapidly-evolving, and increasingly volatile, cyber environment. The TSA administrator's emergency authorities are essential and vital to the Nation's transportation security.

EXAMPLES OF TSA'S CYBERSECURITY PROGRAM

Immediately following a 2021 ransomware incident impacting a major U.S. pipeline company, there was a clear understanding across the administration, Congress, industry, and the public for the need to prevent future pipeline cybersecurity incidents. The administration turned to TSA and the TSA administrator leveraged his authority under 49 U.S.C. § 114 to respond to emerging cyber threats by directing owners and operators of certain pipeline and natural gas facilities to implement a set of select cybersecurity protections to mitigate the threat. The TSA administrator issued 2 SDs in 2021 to immediately address these threats. Among the many requirements, the SDs required pipeline companies to report cybersecurity incidents to CISA within 24 hours after they identify a cybersecurity incident; to designate a cybersecurity coordinator and alternate that is available to TSA around the clock; and to implement specific mitigation measures to protect against ransomware incidents.

Credible cyber threat information also supported the TSA administrator's use of his emergency authority to implement additional security measures to U.S. surface (pipelines and railroads) and aviation (airports and air carriers) transportation networks. In regard to the surface transportation security domain, the cybersecurity SDs require higher-risk pipelines, freight railroads, passenger rail, and rail transit operators to take several critical actions (rail transit operators only require the first 3):

1. Develop and submit to TSA a Cybersecurity Implementation Plan (CIP) to achieve performance-based security outcomes;
2. Develop and maintain an up-to-date Cybersecurity Incident Response Plan (CIRP) to reduce the risk of operational disruption following cybersecurity incidents;
3. Develop and submit to TSA a Cybersecurity Assessment Plan (CAP) to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities; and
4. Develop and submit to TSA an annual report that provides the results of the Cybersecurity Assessment Plan from the previous year.

Within aviation, the TSA administrator used his regulatory authority to amend established security programs of the Nation's largest air carriers and airports to include cybersecurity. Like the surface SDs, these amendments started with requirements to designate a Cybersecurity Coordinator, report cybersecurity incidents to CISA, and to develop a CIRP. They now also include requirements to develop a CIP and CAP and to allow TSA to inspect these documents.

In promulgating these SDs and security program amendments, TSA engaged with stakeholders to enhance understanding of the threat landscape and gather industry feedback. This included stakeholder discussions at the CEO-level with DHS and TSA leadership, Classified threat briefings for industry, multiple policy reviews by industry and Government stakeholders, and consistent engagement sessions with transportation associations and regulated entities for awareness on the proposed strategies. Through these regular engagements with industry partners, we quickly learned that our initial approach to cybersecurity in surface modes was too prescriptive. This approach limited innovation and hindered industry's ability to quickly respond to evolving and emerging dynamic cyber threat landscapes. Based on that feedback, TSA quickly transitioned our regulatory framework in 2022 to an outcome-focused, performance-based model that remains our model to the present day in both surface and aviation modes. This rapid shift to performance-based SDs versus prescriptive SDs demonstrates the flexibility of TSA's emergency authorities and highlights the power of collaboration with our industry partners to collectively address security issues with measures tailored to specific transportation environments.

Since August 2023, TSA also led several in-person and virtual meetings to discuss the pipeline SDs with pipeline owners and operators from various associations and companies. Additionally, TSA hosts a bi-weekly call with the owners and operators subject to the rail SDs to share information and answer questions on the SDs and inspection requirements. Similar calls have begun within the last few months for airports and air carriers. In these engagements, TSA also discusses its cybersecurity policy and strategy, identifies opportunities for improvement, and provides contextual information via the sharing of intelligence and incident information.

Finally, TSA also engages regularly with TSA's Surface Transportation Security Advisory Committee (STSAC) and the Aviation Security Advisory Committee (ASAC) to share and discuss security requirements, issues, and challenges. These statutorily-created committees include representation from the interagency and industry. Whenever able, we will continue to engage with industry partners prior to issuing new security requirements.

Concurrently with these efforts, TSA published a Notice of Proposed Rulemaking (NPRM) that would codify the provisions of the SDs for certain surface modes of transportation into a Cybersecurity Risk Management Program. This proposed rule opened for public comment on November 8, 2024. It continues TSA's commitment to performance-based requirements, builds on TSA's previously-issued cybersecurity requirements from the SDs and seeks to establish a sustainable and comprehensive cyber risk management program for owners and operators that have higher cybersecurity risk profiles. Our routine engagements with stakeholders, as well as coordination with inter-agency partners such as DOT, USCG, and CISA, have been critical in this process—as with the SDs, their feedback has informed decisions on the proposed rule making.

Within the aviation sector, TSA continues to partner with aviation entities on elevating their cybersecurity stance. TSA has partnered and communicated, at the appropriate level based on the maturity of the covered parties, cybersecurity program changes to their cybersecurity programs. As of October 1, 2024, TSA has reviewed and approved over 70 percent of the cybersecurity implementation plans and conducted several inspections of covered parties.

Within the surface modes, all pipeline CIPs have been approved, and nearly all rail plans have been approved. In preparation for the SD CIP inspections, owners and operators were contacted by their Regional Security Director or inspection point of contact well in advance of the inspection to provide details and to coordinate any documentation in advance to ensure all parties were properly prepared. As of May 2024, TSA completed all initial pipeline inspections. By the end of fiscal year 2024, 96 percent of rail inspections have been conducted.

With the approved CIPs in surface, most owners and operators have developed and submitted their CAPs to test the effectiveness of the measures outlined within their CIPs. As of October 23, 2024, TSA has approved 99 percent of pipeline and 45 percent of rail CAPs.

INFORMATION SHARING AND ENGAGEMENT

Our work does not simply end after issuing these cybersecurity requirements. On the contrary, TSA continues its robust stakeholder engagement to mitigate cyber threats. We work closely with covered owners and operators to successfully implement these requirements, educate our vast network of transportation owners and operators, and continue to seek input from both the STSAC and the ASAC on how to best integrate cybersecurity into the fabric of our transportation security mission. TSA conducts extensive outreach with thousands of individual transportation owners and operators to implement these requirements and ensure consistent application across the transportation sector. We continually seek opportunities to expand information exchanges and to provide evaluation tools and training programs to evaluate systems, identify vulnerabilities, and incorporate security measures and best practices that mitigate cyber threats.

On behalf of DHS, TSA and USCG are each a Co-Sector Risk Management Agency for the TSS along with the DOT. In this role, TSA serves with the USCG as the executive agents for developing, deploying, and promoting TSS-focused cybersecurity initiatives, programs, assessment tools, strategies, and threat and intelligence information-sharing products. TSA is in close alignment with CISA and coordinates on both a tactical and strategic level to raise the cybersecurity baseline across the transportation systems sector.

Under the proposed CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule published on April 4, 2024, all entities within the TSS—that are currently required to report to TSA—will also be required to report to CISA. The proposed rule is in line with TSA's SDs and security programs that require certain transportation entities to report cybersecurity incidents, as defined by TSA, to CISA within 24 hours of identification. Regulated entities complying with TSA's requirements will not need to make a duplicate report to CISA; all TSA reporting requirements will occur via a report from TSA into CISA's own systems. Although CIRCIA requirements do not limit TSA's authority to impose cybersecurity reporting requirements, define reportable incidents more broadly than CISA, or impose a time frame for reporting that is shorter than the time frame required by CIRCIA, TSA has ensured that cybersecurity reporting is integrated with the system under development by CISA.

Information and intelligence sharing is a key enabler of TSA's mission to protect the Nation's transportation systems to ensure the freedom of movement for people and commerce. TSA facilitates both Classified and un-Classified briefings for trade associations, industry executive leadership, and key industry security personnel representatives to ensure full understanding of the evolving threat picture. As previously stated, TSA's commitment to information sharing with industry is strongly supported by 2 full-time threat intelligence sharing cells—the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) and the Surface Intelligence Sharing Cell (SISC). Through these entities, TSA shares thousands of threat items, including cyber threat intelligence with cleared stakeholders. These 2 intelligence-sharing cells are excellent examples of Government and industry partnership, and their establishment resulted directly from stakeholder collaboration. Close collaboration with our public and private partners will continue to inform TSA's next steps in the cybersecurity arena.

Finally, we would like to thank Congress and this subcommittee for your support of TSA's transportation security mission and securing the funding for critical cyber resources in fiscal year 2024. The fiscal year 2025 President's budget request, if enacted, will fund specially-trained personnel to accelerate cybersecurity inspection and compliance efforts across the entire TSS. TSA will use the funding to emphasize aviation and surface sector resiliency, use of cyber tools, a trained cyber response staff, a cyber analytical staff, and a regulatory support staff. We recognize the continued need to recruit, train, and retain cybersecurity professionals within TSA. Through recruitment and retention incentives, to include supporting cybersecurity development training opportunities and cybersecurity certifications for personnel, we continue to build our cybersecurity workforce, positioning TSA to effectively tackle the evolving cybersecurity threat as supported by recent budget requests.

Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee, thank you for this opportunity to share the steps and measures TSA has taken in concert with our stakeholders to strengthen transportation critical infrastructure to address the serious and persistent cybersecurity threat. TSA is committed to ensuring appropriate security measures are in place to increase the cybersecurity defenses of our Nation's most critical transportation systems. I look forward to answering any questions you may have.

Mr. GIMENEZ. Thank you, Mr. Lorincz.

I now recognize Mr. Gorman for 5 minutes to summarize his opening statements.

STATEMENT OF CHAD GORMAN, DEPUTY EXECUTIVE ASSISTANT ADMINISTRATOR, OPERATIONS SUPPORT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. GORMAN. Good morning. Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today.

My name is Chad Gorman, and I am the deputy executive assistant administrator for operations support at TSA. In this role, I am responsible for TSA's intelligence operations, regulatory policy, and stakeholder engagement as well as other programs.

I am joined today by deputy executive assistant administrator for security operations, Steve Lorincz. We appreciate the opportunity to discuss TSA's role in cybersecurity for our Nation's transportation infrastructure.

As the Members of this committee know well, cyber attacks are an evolving and persistent threat. Cyber actors, specifically, nation-states like Russia, China, Iran, North Korea—have demonstrated their intent and ability to conduct malicious cyber activity, targeting critical infrastructure by exploiting inherent vulnerabilities of both operational technology and IT systems.

These nation-state threat actors have developed and demonstrated capabilities that pose significant cyber threats to the United States, our critical infrastructure, and the transportation sector.

As the director of national intelligence has stated, our adversaries and strategic competitors have the intent and ability to preposition cyber attack exploits that can be used against U.S. critical infrastructure, including transportation.

In fact, we have observed highly sophisticated activity attributed to the People's Republic of China, assessed as prepositioning for disruptive attacks against U.S. critical infrastructure, including transportation sector, in the event of a major crisis or conflict with the United States.

In response to these urgent threats, the TSA administrator has utilized his emergency authorities found in both statute and regulations, issued security directives, and emergency security program amendments immediately to protect transportation security.

The administrator may use these authorities upon finding that immediate action is necessary to protect transportation security.

The TSA administrator's ability to leverage these unique authorities, and respond immediately during emergency situations had a significantly mitigative threats posed by a rapidly-evolving cyber environment.

These emergency authorities are a vital component of the Nation's—of securing the Nation's transportation system and allow the TSA administrator to act to prevent harm to transportation in the advance of catastrophic consequences.

Following the 2021 cyber incident at a major U.S. pipeline, the TSA administrator leveraged his unique authorities to require transportation and infrastructure stakeholders, both surface and aviation, to implement a variety of cybersecurity protections.

These measures include mandatory reporting of cybersecurity instances, designating a cybersecurity coordinator, requiring high-risk pipeline, freight, railroad, passenger rail, and rail transit operators to develop cybersecurity implementation response and assessment plans and reporting to TSA on their efforts on a recurring basis.

The administrator consulted industry partners regarding these measures and provided multiple threat briefings to CEOs and other industry representatives.

These measures were developed with extensive collaboration with industry stakeholders which allowed TSA to better understand the threat landscape, and gather industry feedback.

It was through this feedback loop that TSA learned that our initial approach to cybersecurity in surface modes was too prescriptive.

Based on that feedback, TSA quickly transitioned our regulatory framework in 2022 to an outcome-focused, performance-based model empowering our industry partners and allowing us collectively to address cybersecurity issues with measures tailored specifically to transportation environments.

Parallel with these emergency measures, TSA continued to pursue more permanent changes through notice-and-comment rulemaking process culminating in the issuance of a Notice of Proposed Rulemaking earlier this month.

This proposed rule is intended to codify the provisions of the recent security directives into a cybersecurity, risk management program.

The proposed rule continues TSA's commitment to performance-based requirements, and builds on TSA's previously-issued cybersecurity requirements aimed at establishing sustainable and comprehensive cyber risk management programs for owners and operators with high-risk profiles.

TSA welcomes and encourages industry comment on this proposed rule. Continuing collaboration with industry partners as well as with interagency partners such as the Cybersecurity and Infrastructure Security Agency, the Department of Transportation, and the United States Coast Guard is critical to securing the Nation's transportation sector from cybersecurity threats.

Industry engagement to date has led directly to better cybersecurity outcomes. TSA is committed to continuing this engagement as these threats evolve.

I want to thank the committee for its interest in cybersecurity of the transportation sector and for its continuing support of TSA and its unique authorities.

I would like to also publicly thank the dedicated employees of TSA for the work they do every day to secure the Nation's transportation systems.

Thank you, Chairman Gimenez and Ranking Member Thanedar, for the opportunity to testify today. We look forward to your questions.

Mr. GIMENEZ. Thank you, Mr. Gorman.

I now recognize Ms. Sherman for 5 minutes to summarize her opening statements.

STATEMENT OF TINA WON SHERMAN, PH D, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT AND ACCOUNTABILITY OFFICE

Ms. SHERMAN. Chairman Gimenez, Ranking Member Thanedar, and Members of the subcommittee, thank you for inviting me to speak with you this morning.

The threat landscape today is not quite what we had envisioned following the tragic events that occurred on September 11.

Current threat assessments cite the increasing prevalence and sophistication of cyber attacks on U.S. critical infrastructure, including on the transportation system sector.

Considered one of the lifeline sectors, transportation systems include aviation and surface modes and moves billions of passengers along with millions of tons of goods every year.

How this sector and others are fundamentally critical to our Nation's economic stability and our everyday lives was brought into clear relief after the ransomware attack on Colonial Pipeline in 2021.

More recently, Volt Typhoon's ability to compromise internet-connected devices in the transportation system sector, as well as other critical infrastructure sectors, have raised significant concerns about the extent of the impact a cyber attack would have on the United States if carried out as part of a major conflict by a foreign adversary.

The agency I represent, GAO, included the cybersecurity of critical infrastructure as part of its high-risk list over 20 years ago, and since that time, we have made numerous recommendations on cybersecurity in the transportation system sector.

For example, in 2019, 2 years before Colonial Pipeline, we reported on weaknesses in TSA's management of its pipeline security efforts. Since that time, TSA has implemented all but one of our recommendations.

The remaining recommendation is for TSA to update its 2010 Pipeline Security and Incident Recovery Protocol Plan, to ensure the plan reflects laws, policies, and changes in pipeline security threats, such as cybersecurity.

TSA officials told us they anticipate completion of the updated protocol plan by July of next year.

TSA has used its various statutorily-granted authorities to help secure all modes of the transportation system. This includes issuing security directives and emergency amendments in response to threats, events, or significant vulnerabilities, as well as recently initiating a rule making to develop cybersecurity regulations for freight and passenger rail, pipelines, and more limitedly, over-the-road buses.

Over the past 5 years, GAO has reviewed TSA security directives and emergency amendments in both aviation and surface transportation systems, and has made recommendations to clarify the process for renewing such directives and amendments, and for obtaining and documenting stakeholder input.

We also recently reported that TSA was unable to demonstrate that its security directives and emergency amendments align with leading practices for ransomware.

As it moves through its rule-making process for surface transportation, TSA should consider leading practices GAO has identified to improve the effectiveness of the process, including incorporating project management practices, such as timely communication with external stakeholders about the rule making's process and progress as well as other details.

TSA should also be prepared to address some of the factors that can delay rule making, such as the complexity of the issues covered, shifts in administration and agency priorities, and the availability of resources to carry out a rule making.

In closing, TSA must be positioned to effectively mitigate cybersecurity threats to ensure the safe movement of people and goods across our Nation's transportation system.

GAO will continue to assist Congress in the oversight of TSA's efforts.

I'd like to thank my GAO colleagues for their tremendous support in my preparation and to the subcommittee for holding this hearing.

[The prepared statement of Ms. Sherman follows:]

Prepared Statement of Tina Won Sherman

Tuesday, November 19, 2024

GAO HIGHLIGHTS

Highlights of GAO–25–107947, a testimony before the Subcommittee on Transportation and Maritime Security, Committee on Homeland Security, House of Representatives.

Why GAO Did This Study

Surface transportation comprises multiple modes—freight rail, passenger rail, and pipelines—and moves billions of passengers and millions of tons of goods each year. Domestic and foreign adversaries likely will continue to threaten the integrity of our Nation's critical infrastructure, including the transportation systems sector. They perceive targeting these sectors would have cascading negative impacts on U.S. industries and citizens, according to a DHS threat assessment.

This statement discusses GAO's portfolio of work on TSA's efforts to enhance cybersecurity and its progress addressing prior GAO recommendations.

This statement is based on prior GAO reports issued from December 2018 through July 2024, along with selected updates on TSA's efforts to enhance cybersecurity and its progress addressing previous GAO recommendations. For these reports and selected updates, GAO reviewed TSA documentation, analyzed data, and interviewed agency officials.

What GAO Recommends

GAO made 6 recommendations to DHS or TSA to address cybersecurity issues related to the transportation systems sector in the reports covered by this statement. DHS or TSA concurred with all of them. As of November 2024, DHS or TSA implemented 1 recommendation, partially addressed 1 recommendation, and has not implemented 4 recommendations. GAO will continue to monitor the agency's progress.

SURFACE TRANSPORTATION.—TSA IS TAKING STEPS TO ENHANCE CYBERSECURITY, BUT ADDITIONAL ACTIONS ARE NEEDED

What GAO Found

The Transportation Security Administration (TSA)—a component within the Department of Homeland Security (DHS)—is responsible for security in the Nation's transportation systems. To fulfill that responsibility, TSA has statutory authority to issue security directives imposing requirements on industry without providing notice or the opportunity for public comment.

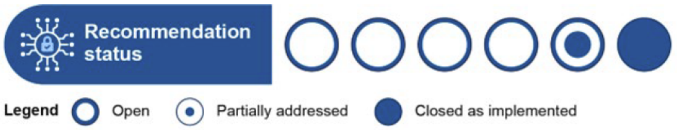
In July 2021, GAO reported that in May 2021, TSA began issuing security directives pursuant to this authority in response to a ransomware attack on a U.S. pipeline company. TSA has issued, revised, and extended 5 security directives requiring various actions to mitigate cyber threats in the freight rail, passenger rail, and pipeline modes. According to TSA, it has done so with industry feedback and Federal oversight approval.

In November 2024, TSA issued a Notice of Proposed Rulemaking that, according to TSA, builds on the agency's performance-based cybersecurity requirements issued via security directives since 2021. TSA stated that this rule proposes to mandate cyber risk management and reporting requirements for certain surface transportation owners and operators.

In prior work, GAO identified various challenges to cybersecurity in the transportation systems sector. For example, in January 2024, GAO reported that ransomware was having increasingly devastating impacts in the sector and found that TSA's security directives did not align with ransomware leading practices. GAO recommended that DHS determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. As of November 2024, this recommendation was not yet implemented.

In addition, in December 2022, GAO found that TSA had taken steps to enhance the cybersecurity of internet-connected devices in the transportation systems sector. However, TSA had not developed metrics to measure the effectiveness of their efforts or conducted sector-wide cybersecurity risk assessments specific to these devices. GAO recommended that TSA develop a sector-specific plan that includes these metrics and include internet-connected devices in such sector-wide assessments. As of November 2024, these recommendations were not yet implemented.

Status of GAO Recommendations to DHS or TSA to Improve Surface Transportation Cybersecurity, as of November 2024



Source: GAO analysis; Icons-Studio/stock.adobe.com (icon). | GAO-25-107947

Chairman Gimenez, Ranking Member Thanedar, and Members of the subcommittee: I am pleased to be here today to discuss our work on the Transportation Security Administration's (TSA) efforts to address cybersecurity issues. TSA—a component within the Department of Homeland Security (DHS)—has a stated mission to protect the Nation's transportation systems to ensure freedom of movement for people and commerce.

Within the transportation systems sector, surface transportation comprises multiple modes of transportation—freight rail, passenger rail, and pipelines—and moves billions of passengers and millions of tons of goods each year. DHS's 2024 Homeland Threat Assessment noted that domestic and foreign adversaries likely will continue to threaten the integrity of our Nation's critical infrastructure—including the transportation systems sector—over the next year, in part because they perceive targeting these sectors would have cascading impacts on U.S. industries and citizens.[1]

My statement today discusses GAO's portfolio of work on TSA's efforts to enhance cybersecurity and its progress addressing our recommendations. This statement is based on prior GAO reports issued from December 2018 through July 2024, along with selected updates on TSA's efforts to enhance cybersecurity and its progress addressing the recommendations from those prior reports.[2] To conduct work on our prior reports and selected updates, we reviewed TSA documentation, analyzed data, and interviewed agency officials.

More detailed information on the objectives, scope, and methodologies of our prior work can be found in each of the reports cited in this statement. We conducted the work on which this statement is based in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

Cyber Threats to the Transportation Systems Sector

Cyber threats to critical infrastructure sectors that rely on electronic systems and data to support their missions continue to increase and represent a significant national security challenge. A variety of threat actors can carry out cyber attacks on critical infrastructure, including transportation systems. Examples of these threat actors include nations, criminal groups, terrorists, and insiders. The 2024 Annual Threat Assessment of the U.S. intelligence community stated that China, Iran, North Korea, and Russia posed the greatest cybersecurity threats to U.S. critical infrastructure.[3] The assessment stated that these countries possessed the ability to launch cyber attacks that could have disruptive effects on U.S. critical infrastructure.

Illustrating this threat, in February 2024, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation, National Security Agency, TSA, and other Federal and international partners issued a joint advisory stating that Chinese-sponsored cyber actors from a group known as Volt Typhoon were seeking to pre-position themselves on IT networks to carry out cyber attacks in the event of a major crisis or conflict with the United States.[4]

Specifically, Federal officials found that Volt Typhoon had compromised IT systems in the transportation systems sector and other critical infrastructure sectors, including communications, energy, and water and wastewater systems. The alert stated that Federal officials had a high degree of confidence that the attackers would be able to move from IT networks to operational technology assets and disrupt critical functions.

[1] Department of Homeland Security, Office of Intelligence and Analysis, Homeland Threat Assessment 2024, 23–333–IA (Sept. 14, 2023), accessed Nov. 13, 2024, *https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf.*

[2] Those prior GAO reports are cited in this statement.

[3] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (Feb. 5, 2024), accessed on Nov. 13, 2024, *https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.*

[4] CISA, *Cybersecurity Advisory: PRC [People's Republic of China] State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,* AA24–038A (February 2024), accessed Nov. 13, 2024, *https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.* CISA and its U.S. and international partners previously issued an alert in May 2023 after detecting Volt Typhoon hacking into critical infrastructure in Guam, which is home to 3 U.S. military bases. Microsoft, which first detected the hacking, noted that the operation's likely aim was to disrupt critical communications between the United States and Asia region during a future crisis.

Federal Cybersecurity Challenges

In June 2024, we reiterated the importance of addressing 4 major cybersecurity challenges, one of which is protecting the cybersecurity of critical infrastructure.[5] With regard to protecting the cybersecurity of critical infrastructure, we reported that more work remains. Specifically, we made 126 recommendations in public reports since 2010 in this area. While Federal agencies have implemented 62 of these recommendations, they have not fully implemented 64 of them as of May 2024.

In addition, we reported in January 2024 that the Federal agencies responsible for 4 critical infrastructure sectors that reported almost half of all ransomware attacks—critical manufacturing, energy, health care and public health, and transportation systems—had not determined the extent of their adoption of leading practices to address ransomware.[6]

Sector Risk Management Agencies and TSA's Transportation Systems Sector Responsibilities

Sector Risk Management Agencies (SRMAs) are Federal departments or agencies, designated by law or Presidential directive, with specific responsibilities for their designated critical infrastructure sectors.[7] SRMAs coordinate with CISA to provide specialized expertise to critical infrastructure owners and operators as well as to support programs and activities for their relevant sector. In carrying out these activities, SRMAs are to coordinate with DHS, other Federal agencies, as appropriate, and State, local, Tribal, and territorial partners. They also are to collaborate with critical infrastructure owners and operators within their sectors. National Security Memorandum–22, issued in April 2024, further defined SRMA roles and responsibilities, such as leading sector risk management activities, which, according to the Memorandum, should include recommending sector-specific measures to protect critical infrastructure.[8]

TSA is 1 of DHS's 2 designated agencies that fulfills DHS's SRMA responsibilities for the transportation systems sector.[9] The Department of Transportation is designated as a co-lead for the transportation systems sector. In TSA's role working with the transportation systems sector, it has lead responsibility for coordinating critical infrastructure protection efforts within various surface modes of transportation, including pipelines, freight rail, and mass transit.

TSA'S CYBERSECURITY DIRECTIVES REQUIRE ACTIONS TO MITIGATE CYBER THREATS ACROSS THE SURFACE TRANSPORTATION SECTOR

TSA is responsible for security in the Nation's transportation systems. To fulfill that responsibility, TSA has statutory authority to issue security directives imposing requirements on industry without providing notice or the opportunity for public comment where the administrator determines that a directive must be issued immediately to protect transportation security.[10] In July 2021, we reported that in May 2021, TSA began issuing security directives pursuant to this authority in response to the Colonial Pipeline ransomware attack.[11]

As shown in the table below, since 2021, TSA has issued 5 security directives requiring various actions to mitigate cyber threats in the freight rail, passenger rail, and pipeline modes. TSA has revised and extended each of these directives several times. According to TSA documentation, the agency has done so with industry

[5] GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation,* GAO–24–107231 (Washington, DC: June 13, 2024). We reported that the Federal Government needed to address 4 major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing Federal systems and information, (3) protecting the cybersecurity of critical infrastructure, and (4) protecting privacy and sensitive data. Within these 4 challenges are 10 actions critical to successfully dealing with the serious cybersecurity threats facing the Nation.

[6] GAO, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support,* GAO–24–106221 (Washington, DC: Jan. 30, 2024).

[7] 6 U.S.C. § 650(23). Although sector-specific plans identify specific departments, agencies, or components within departments or agencies as having lead or co-lead responsibilities for carrying out critical infrastructure protection activities, other offices within the SRMA departments and agencies also support sector critical infrastructure protection efforts.

[8] White House, National Security Memorandum on Critical Infrastructure Security and Resilience, National Security Memorandum–22 (Washington, DC: April 30, 2024), accessed Nov. 13, 2024, *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/*.

[9] The U.S. Coast Guard is also designated to fulfill DHS's SRMA responsibilities for the transportation systems sector, primarily for maritime security.

[10] 49 U.S.C. § 114(I)(2)(A).

[11] GAO, *Critical Infrastructure Protection: TSA Is Taking Steps to Address Some Pipeline Security Program Weaknesses,* GAO–21–105263 (Washington, DC: July 27, 2021).

stakeholder input and feedback. An interagency oversight body has also reviewed and approved these directives after issuance.[12] Of the 5 directives, 3 directives have requirements, such as cybersecurity incident reporting, to enhance cybersecurity in each transportation mode. The remaining 2 directives impose additional requirements for cybersecurity mitigation actions and testing across the modes.

[12] The Transportation Security Oversight Board, within DHS, is statutorily required to review and ratify or disapprove any security directives issued by TSA within 30 days. 49 U.S.C. §§ 114(l)(2)(B), 115(c)(1). The board is composed of 7 members from the Departments of Defense, Justice, Homeland Security, Transportation, and the Treasury, the National Security Council, and the Office of the Director of National Intelligence.

TABLE 1: TRANSPORTATION SECURITY ADMINISTRATION'S (TSA) SECURITY DIRECTIVES ON SURFACE TRANSPORTATION CYBERSECURITY FROM MAY 2021 THROUGH OCTOBER 2024

Title	Description	Effective date	Expiration date
Security Directive Pipeline–2021–01 Enhancing Pipeline Cybersecurity (SD–01).	Requires critical pipeline owners and operators to designate a cybersecurity coordinator, report cybersecurity incidents, and conduct a vulnerability assessment.	May 28, 2021	May 28, 2022.
Current version is SD–01D	Revisions have included an updated definition of a cybersecurity incident, an increased time to report incidents from 12 to 24 hours, and a requirement for operators to test and evaluate cybersecurity implementation plans.	May 29, 2024	May 29, 2025.
Security Directive Pipeline–2021–02 Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing (SD–02).	Requires critical pipeline owners and operators to implement mitigation actions to protect against ransomware attacks and other known threats, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review.	July 26, 2021	July 26, 2022.
Current version is SD–02E	Revisions have included changes to requirements to provide flexibility in meeting intended security outcomes.	July 27, 2024	July 27, 2025.
Security Directive 1580–21–01 Enhancing Rail Cybersecurity (SD–03).	Requires freight railroads owners and operators to designate a cybersecurity coordinator, report cybersecurity incidents, and conduct a vulnerability assessment.	Dec. 31, 2021	Dec. 31, 2022.
Current version is SD–03C	Revisions have included clarification of the entities to which it applies and additional cybersecurity incident response plan exercise requirements.	Oct. 24, 2024	Oct. 24, 2025.
Security Directive 1582–21–01 Enhancing Public Transportation and Passenger Railroad Cybersecurity (SD–04).	Requires public transportation and passenger railroad owners and operators to designate a cybersecurity coordinator, report cybersecurity incidents, and conduct a vulnerability assessment.	Dec. 31, 2021	Dec. 31, 2022.
Current version is SD–04C	Revisions have included clarification of the entities to which it applies and additional cybersecurity incident response plan exercise requirements.	Oct. 24, 2024	Oct. 24, 2025.

Security Directive 1582 Rail Cybersecurity Mitigation Actions and Testing (SD–05).	Requires certain railroad owners and operators to establish a TSA-approved plan to implement cybersecurity measures and a program to annually assess the effectiveness of these measures.	Oct. 24, 2022	Oct. 24, 2023.
Current version is SD–05C	Revisions include adding new requirements for assessing, updating, and reporting assessments of cybersecurity measures.	July 1, 2024	May 2, 2025.

Source: GAO analysis of TSA documentation./GAO–25–107947.

In November 2024, TSA issued a Notice of Proposed Rulemaking titled Enhancing Surface Cyber Risk Management in the *Federal Register.*[13] According to TSA, this proposed rule builds on the agency's performance-based cybersecurity requirements issued via security directives since 2021.[14] TSA stated that this rule proposes to mandate cyber risk management and reporting requirements for certain surface transportation owners and operators. TSA is proposing to impose cyber risk management requirements on certain pipeline and rail owner and operators. TSA is also proposing a requirement on pipeline facilities and systems to have a physical security coordinator and report significant physical security concerns.[15] TSA is further proposing to impose a limited requirement on certain over-the-road bus owner and operators to report cybersecurity incidents.

TSA is requesting comments on, among other things, the impacts of regulations and requirements as well as existing training and certification programs. Specifically, TSA is requesting comments on the impact of regulations and requirements being imposed by other Federal, State, and local entities, including DHS components, and potential options for regulatory harmonization. In addition, TSA is requesting comments on existing training and certification programs that could provide options to meet proposed qualification requirements for cybersecurity coordinators.[16] TSA plans to review and provide them as examples, as appropriate, to owners and operators that would be subject to these requirements. The public comment period is 90 days, or until February 5, 2025.

TSA's proposed rule is a recent example of a Federal effort to put forth requirements to mitigate and report cyber attacks. This includes DHS's efforts to harmonize cyber incident reporting requirements by certain entities through the rulemaking process.[17] Given the array of existing requirements for cybersecurity, we testified in June 2024 on the importance of regulatory harmonization—the development and adoption of more consistent standards and regulations for cybersecurity.[18] Without harmonization, adverse impacts can occur. For example, we reported in 2020 that 4 Federal agencies had established cybersecurity requirements for States to follow in securing data.[19] However, these requirements had conflicting parameters such as the number of unsuccessful log-on attempts prior to locking out users. TSA's rulemaking effort presents an opportunity for the agency to avoid similar pitfalls by considering and, where appropriate, aligning with existing Federal cybersecurity requirements.

TSA TOOK STEPS TO IMPROVE CYBERSECURITY, BUT ADDITIONAL ACTION IS NEEDED

Since 2018, we have made 6 recommendations to DHS or TSA to address cybersecurity issues related to the transportation systems sector. DHS or TSA concurred with all the recommendations. As of November 2024, DHS or TSA implemented 1 recommendation, partially addressed 1 recommendation, and has not implemented 4 recommendations. Specifically, as shown in table 2, TSA developed a workforce plan to better account for cybersecurity workforce needs, but additional action is needed to improve ransomware resilience in the transportation systems sector and to update aged pipeline recovery protocols.

[13] *Enhancing Surface Cyber Risk Management,* 89 Fed. Reg. 88,488 (proposed Nov. 11, 2024) (to be codified at 49 C.F.R. Parts 1500, 1503, 1520, 1570, 1580, 1582, 1584, and 1586), accessed Nov. 13, 2024, *https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management.*

[14] TSA, *TSA Announces Proposed Rule that Would Require the Establishment of Pipeline and Railroad Cyber Risk Management Programs,* Press Release (Washington, DC: Nov. 6, 2024), accessed Nov. 13, 2024, *https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and.*

[15] According to TSA's proposed rule, a Physical Security Coordinator is a designated point of contact at the corporate level to function as the administrator for sharing security-related activities and information.

[16] Cybersecurity Coordinators are designated points of contact for TSA to convey time-sensitive information about threats or security procedures to an owner or operator.

[17] DHS's CISA submitted a proposed rule related to cyber incident reporting requirements to the *Federal Register* in March 2024, and it was published in April 2024. DHS plans to issue the final rule by October 2025. For more information, see *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements,* 89 Fed. Reg. 23,644 (proposed Apr. 4, 2024) and GAO, *Critical Infrastructure Protection: DHS Has Efforts Underway to Implement Federal Incident Reporting Requirements,* GAO–24–106917 (Washington, DC: July 30, 2024).

[18] GAO, *Cybersecurity: Efforts Initiated to Harmonize Regulations, but Significant Work Remains,* GAO–24–107602 (Washington, DC: June 5, 2024).

[19] GAO, *Cybersecurity: Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States,* GAO–20–123 (Washington, DC: May 27, 2020).

TABLE 2: GAO RECOMMENDATIONS TO THE DEPARTMENT OF HOMELAND SECURITY OR TRANSPORTATION SECURITY ADMINISTRATION FORIMPROVEMENTS TO TRANSPORTATION SYSTEMS SECTOR CYBERSECURITY, AS OF NOVEMBER 2024

GAO Report Area and Year	Recommendation summary	Status
Ransomware risk reduction 2024[1].	Determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware.	Open.
	Develop and implement routine evaluation procedures that measure the effectiveness of Federal support in helping reduce the risk of ransomware to the transportation systems sector.	Open.
Securing internet-connected devices 2022[2].	For the transportation systems sector, develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts to enhance the cybersecurity of their sector's internet of things and operational technology environments.	Open.
	For the transportation systems sector, to include internet of things and operational technology devices as part of the risk assessments of their sector's cyber environment.	Open.
Pipeline security recovery protocols 2019[3].	Update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes in pipeline security threats, technology, Federal law and policy, and any other factors relevant to the security of the Nation's pipeline systems.	Partially addressed.
Pipeline cybersecurity workforce 2018[4].	Develop a strategic workforce plan, including the number of personnel necessary to meet goals set for the Pipeline Security Branch, as well as the knowledge, skills, and abilities, including cybersecurity, required.	Closed as implemented.

Source: GAO/GAO–25–107947.

[1] GAO, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support,* GAO–24–106221 (Washington, DC: Jan. 30, 2024).

[2] GAO, *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices,* GAO–23–105327 (Washington, DC: Dec. 1, 2022).

[3] GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment,* GAO–19–426 (Washington, DC: June 5, 2019).

[4] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management,* GAO–19–48 (Washington, DC: Dec. 18, 2018).

Below are examples of our past findings and related recommendations to improve transportation systems sector cybersecurity.

Pipeline cybersecurity workforce.—In December 2018, we found that TSA had not established a workforce plan for its Pipeline Security Branch that identified staffing needs or cybersecurity skills required to best implement pipeline security reviews.[20] We recommended that TSA develop a strategic workforce plan that outlines the knowledge, skills, and abilities, including those related to cybersecurity, needed to effectively conduct the reviews. Subsequently, we designated the recommendation as a priority for DHS implementation.[21]

TSA completed a Workforce Assessment Report in May 2021 that identified, among other things, several staffing inadequacies, particularly related to the pipeline cybersecurity mission. Specifically, the Assessment Report highlighted that the organization lacked qualified personnel with relevant skills, appropriate certifications, or expertise in cybersecurity and that over one-third of the agency's position descriptions were improperly classified for the duties required. The Workforce Assessment Report included a recommended workforce plan that defined short-term and long-term initiatives for addressing staffing inadequacies. For example, the workforce plan listed initiatives for developing and codifying specific staff duties required for physical or cybersecurity. These actions helped ensure that TSA was able to meet its mission of reducing pipeline systems' vulnerabilities to cybersecurity risks, especially in a dynamic and evolving threat environment.

Pipeline security recovery protocols. In June 2019, we found that TSA's Pipeline Security and Incident Recovery Protocol Plan, issued in March 2010, defined the roles and responsibilities of Federal agencies and the private sector, among others, related to pipeline security incidents.[22] For example, in response to a pipeline incident, TSA coordinates information sharing between Federal and pipeline stakeholders, and Department of Transportation's Pipeline and Hazardous Materials Safety Administration coordinates Federal activities with an affected pipeline operator to restore service. However, TSA had not revised the plan to reflect changes in several areas, including cybersecurity.

We recommended that TSA update the 2010 Pipeline Security and Incident Recovery Protocol Plan to ensure the plan reflects relevant changes in pipeline security threats, specifically cybersecurity. As of November 2024, TSA officials reported that the Protocol Plan is being revised to bring it into conformity with several national-level policy documents, such as the National Response Framework, the National Cybersecurity Incident Response Plan, and the National Terrorism Advisory System. The officials stated that they anticipate completion of the updated Protocol Plan by end of July 2025.

In May 2021, the Colonial Pipeline Company learned that it was a victim of a cyber attack, and malicious actors reportedly deployed ransomware against the pipeline company's business systems. To prevent further compromise, the company temporarily halted all pipeline operations, leading to gasoline shortages throughout the southeast United States. This example highlights the importance of having response plans and protocols in place for responding to cybersecurity incidents in the sector.

Internet of things and operational technology risk reduction.—In December 2022, we found that TSA had taken steps to enhance the cybersecurity of the transportation systems sector's internet of things[23] and operational technology[24] environments.[25] For example, TSA issued threat briefings specific to operational technology and published a Surface Transportation Cybersecurity Toolkit designed to provide informative cyber risk management tools and resources. Additionally, as discussed above, TSA issued security directives for higher-risk railroads and rail transit and

[20] GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management,* GAO–19–48 (Washington, DC: Dec. 18, 2018).

[21] GAO, *Priority Open Recommendations: Department of Homeland Security,* GAO–20–355PR (Washington, DC: Apr. 23, 2020). Priority recommendations are those that GAO believes warrant priority attention from heads of key departments or agencies. They are highlighted because their implementation could save large amounts of money; improve Congressional and/or Executive branch decision making on major issues; eliminate mismanagement, fraud, and abuse; or ensure that programs comply with laws and funds are legally spent, among other benefits.

[22] GAO, *Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment,* GAO–19–426 (Washington, DC: June 5, 2019).

[23] Internet of things generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or "things," throughout such places as buildings, vehicles, transportation infrastructure, or homes.

[24] The National Institute of Standards and Technology defines operational technology as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

[25] GAO, *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices,* GAO–23–105327 (Washington, DC: Dec. 1, 2022).

pipeline owners and operators that require certain actions to improve cybersecurity preparedness. The actions include appointment of cybersecurity coordinators, reporting of cybersecurity incidents to CISA, conducting a cybersecurity vulnerability assessment, and development of cybersecurity incident response plans.[26]

However, TSA had not developed qualitative or quantitative metrics to measure the effectiveness of their efforts. In addition, TSA and the co-sector risk management agencies (U.S. Coast Guard and Department of Transportation) had not conducted sector-wide cybersecurity risk assessments specific to internet of things and operational technology devices. We recommended that TSA along with the co-sector risk management agencies develop a sector-specific plan that includes metrics for measuring the effectiveness of their efforts and include internet of things and operational technology devices as part of risk assessments of their sector's cyber environment. As of November 2024, these recommendations were not yet implemented.

Ransomware risk reduction. In January 2024, we reported that ransomware—software that makes data and systems unusable unless ransom payments are made—was having increasingly devastating impacts.[27] We found that TSA required owners and operators of freight and passenger rail, pipelines, public transportation, and surface transportation to implement certain cybersecurity measures as a protection against malicious cyber intrusions. However, we also found that TSA, and other SRMAs, had not fully assessed the effectiveness of their ransomware-related support. Therefore, we recommended that DHS develop and implement routine evaluation procedures that measure the effectiveness of Federal support in helping reduce the risk of ransomware to the transportation systems sector.

In addition, we found that TSA's security directives for freight and passenger rail, pipelines, and public transportation did not align with National Institute of Science and Technology's Ransomware leading practices. We recommended that DHS determine the extent to which the transportation systems sector is adopting leading cybersecurity practices that help reduce the sector's risk of ransomware. As of November 2024, these recommendations were not yet implemented.

Chairman Gimenez, Ranking Member Thanedar, and Members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

Mr. GIMENEZ. Thank you, Ms. Sherman. Members will be recognized by order of seniority for their 5 minutes of questioning.

I now recognize myself for 5 minutes of questioning.

Back to you, Ms. Sherman, this 300-page document, what do you consider that? Is it more check-the-box reporting requirements, or does it actually help industry in protecting itself from cyber attacks?

Ms. SHERMAN. While we haven't done an in-depth analysis of the recent rule making, we know that there's a number of the requirements that are carried over from the existing security directives, intended to help, of course, improve the cybersecurity of surface transportation.

We also think that training that's to be—potentially to be implemented that's included as part of the rule making is a positive step forward.

Deterrence is always really difficult, of course, to measure, but we do see this as an important step forward by TSA.

Mr. GIMENEZ. Mr. Gorman, in terms of the rule making itself, I mean, I'm—you know, as you were speaking, I'm looking at—let's

[26] Department of Homeland Security, Transportation Security Administration, *Enhancing Rail Cybersecurity,* Security Directive 1580–21–01 (Springfield, VA: Dec. 31, 2021), accessed Nov. 13, 2024, *https://www.tsa.gov/sites/default/files/sd-1580-21-01__signed.pdf; Enhancing Public Transportation and Passenger Railroad Cybersecurity,* Security Directive 1582–21–01, (Springfield, VA: Dec. 31, 2021), accessed Nov. 13, 2024, *https://www.tsa.gov/sites/default/files/sd-1582-21-01__signed.pdf; Revision to the Security Directive Pipeline–2021–02 series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing,* Security Directive Pipeline–2021–02C (Springfield, VA: July 27, 2022), accessed Nov. 13, 2024, *https://www.tsa.gov/sites/default/files/tsa__sd__pipeline-2021-02-july-21__2022.pdf;* and *Enhancing Pipeline Cybersecurity,* Security Directive Pipeline–2021–01B (Springfield, VA: May 29, 2022), accessed Nov. 13, 2024, *https://www.tsa.gov/sites/default/files/sd__pipeline-2021-01b__05-29-2022.pdf.*

[27] GAO–24–106221.

focus, say, on rail. OK? So much of this country's commerce, energy, et cetera, runs on rails.

How much of our infrastructure now is interconnected and dependent on electronic systems for switching, scheduling, et cetera, you know, making sure that that train is on this track at this time, et cetera, et cetera? How much of that is automated? How much of it is really susceptible to a cyber attack?

Mr. GORMAN. Specifically in the rail environment?

Mr. GIMENEZ. Yes.

Mr. GORMAN. So I don't have an exact number for you, Chairman, but it is a large portion, particularly with the enactment of systems like mandatory positive train control, and the interconnectedness there of the rail network.

It is a Federal requirement that those rail entities actually have that system in operation for safety purposes, and so that system, as well as things like switching and others, are what provided TSA the methodology by which we scoped in those rail entities that you see within the NPRM language, particularly those class I rail entities that provide the bulk of the movement for the goods and services that you just referenced, sir, as well as a small amount of short line and regional railroads that, while of a smaller entity size, provide critical functions to the function of the overall system, or provide critical national security functions in the rail environment that we deemed as necessary for the protection of this rule.

Mr. GIMENEZ. How vulnerable are we to, say, a massive cyber attack on our rail system that basically paralyzes our rail system in the United States?

Mr. GORMAN. I think it varies across the system, sir, and these measures particularly are meant to raise the cyber resiliency of both rail, pipeline, and other entities that fall within the scope, and built off of specifically industry standards as listed in things like existing NIST Cybersecurity Frameworks, as well as CISA's recent cybersecurity performance goals to make sure that we are continuing to raise the bar for cybersecurity, particularly in these critical assets in transportation.

Mr. GIMENEZ. But no matter how much you raise the bar for cybersecurity, this is a constant game of one-upmanship, right, and eventually, if somebody really wants to penetrate it, eventually you have to account for the eventuality of us losing that or somebody penetrating the system and wreaking havoc on the United States.

In these rules, do you account for that, and do you mandate resiliency so that, worst-case scenario, you have to get off the grid, will we be able to still transport goods and services by the old method? Or are we so reliant on the new method that we've forgotten the old method, and we'll be basically stuck in gridlock?

Mr. GORMAN. So given the dynamic nature of the cybersecurity threat that we face now and we anticipate facing in the future, I think there's 3 primary areas of this rule that are germane to your question.

First, we learned, based on the performance of the requirements that are existing in our current issued SDs, of a performance-based model is the model to move into, both now and into the future.

These requirements that we have in the NPRM as posted, we believe, have—provide both specificity in the outcomes that we are requiring, as well as flexibility for operators to adapt those to their specific operations, systems, and technologies to achieve those, as well as our overall goal is to prevent the disruption of critical services.

So as we are looking to work with industry, we drive these requirements at those critical assets that are determined within their operations.

Third, we are mandating that these owner-operators develop, maintain, and regularly exercise response plan, particularly for potential incidents that may occur on and directly to their networks, to provide redundancy and ability to quickly respond and recover from those instances.

Mr. GIMENEZ. Thank you. My time is up.

I now recognize the Ranking Member, Mr. Thanedar, for 5 minutes.

Mr. THANEDAR. I thank the Chairman.

Mr. Lorincz and Mr. Gorman, in the aftermath of the Colonial Pipeline attack, Congress has consistently supported TSA's request for additional cybersecurity resources and personnel.

For fiscal year 2025, the Biden-Harris administration has requested an additional $8 million and 41 positions for TSA cybersecurity activities.

How will that funding and those positions be used to enhance TSA's efforts, and what more does TSA need from Congress to further advance transportation cybersecurity?

Mr. LORINCZ. Thank you for that question. First of all, I think it's really important to acknowledge the support that we have received and continue to receive, and we're very, very appreciative of that.

Currently, in the aviation sector, we have oversight of 168 entities. In the surface sector, we have oversight of 155, and that's going to also grow moving into next year.

The resource allocation, the 41 positions that you alluded to is going to help tremendously as we continue to move forward.

Currently within our security operation structure for both aviation, we have 32 employees that are allocated to provide support for those 168 entities. So as you could tell, the scope of the work is great, especially with some of the requirements and some of the pivoting that we have done based on industry feedback.

I just want to share one of those things. So industry has been instrumental in building this partnership and support with TSA, and they requested a couple things which we worked with them on.

One is to not submit their information to us. So our inspection time line went from 2 days to maybe a week, so that drives additional resources.

Also within the surface sector, we have about 60 employees that are allocated to handle about 155 entities.

So the workload is there, but we truly appreciate the support that we continue to receive, and we look forward to also the President's budget which identifies these positions. Thank you.

Mr. GORMAN. I would add one more thing to Mr. Lorincz's response there as well is that we also have critical responsibilities, as a sector risk management agency, to not only regulate within this space, but then also specifically to provide support to the industry stakeholders, both in the surface and aviation domains.

These resources would also provide greater ability for us to engage on a regular, repeating basis with our industry stakeholders as they both implement these measures but also face cybersecurity threats directly at their networks, as well as provide actionable intelligence directly to CIOs and CISOs within these companies' structures, so they can help best guide threat-hunting teams and other preparatory measures above and beyond those measures that are required to additionally provide protections across transportation.

Mr. THANEDAR. Thank you.

Now, at times, we have heard complaints about TSA's use of, and reliance on, security directives.

However, statute requires the TSA administrator to immediately issue a security directive whenever the administrator determines that doing so is necessary to protect transportation security.

The authority to issue security directives allows the TSA administrator to respond quickly and effectively to imminent threats. The regulatory process is simply not always fast enough to keep up with the evolving intelligence landscape.

My question is, how critical is TSA's security directive authority to the agency's ability to carry out its mission?

Aside from TSA's recent cybersecurity efforts, how else has TSA used the security directives to protect transportation security?

If TSA had not moved immediately following the Colonial Pipeline attack to issue cybersecurity directives across several transportation modes, would our transportation sector have been left vulnerable to additional attacks?

Mr. GORMAN. So to answer your first question—thank you for the question—we believe that the administrator's emergency authorities are vital to the security of the transportation sector.

We have used these authorities both, as you've mentioned here in this hearing, on several instances over the last several years, to ensure that we were rapidly responding to the ever-persistent and then direct threats posed by our cybersecurity adversaries.

With regards to other instances beyond cybersecurity, we would be happy to provide the Members a listing of that as that information is sensitive security information, and we cannot discuss those details here in this hearing. But we will be able to follow up with you directly after this hearing to provide you a summary of several examples of their uses.

Mr. THANEDAR. Thank you, and I yield back.

Mr. GIMENEZ. Thank you to the Ranking Member.

I now recognize the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Lorincz, you are the deputy executive assistant administrator for security operations for TSA under the United States Department of Homeland Security, correct?

Mr. LORINCZ. That's correct.

Mr. HIGGINS. Mr. Gorman, you are the deputy executive assistant administrator for operations support with TSA under the DHS, correct?

Mr. GORMAN. Correct.

Mr. HIGGINS. OK. So just so America knows, we got two of the honchos here in front of us as it relates to TSA regulations and the effort to introduce security enhancements for our industry partners that fall under the jurisdictional authority of TSA like our stakeholders running rail and pipelines, in an effort to protect our Nation's infrastructure from cyber threat.

Largely, Americans feel quite vulnerable from cyber threat. From sea to shining sea, we do not—we are not reassured by what we read in the news every day about a major cyber breach in this industry, a major cyber breach from that massive bank, another major cyber breach in this large Government entity.

Americans generally get it, that this thing is a moving target, and it is a serious threat, and we, as a Nation, we have to respond. So TSA has its role to play, and Congress has given the Transportation Security Administration the authority to issue what are called security directives. Is that correct, gentlemen?

Mr. GORMAN. That is correct.

Mr. LORINCZ. Yes, correct.

Mr. HIGGINS. OK. So in that time frame, which is recent history, since 2021, in the effort, as a Nation, to respond to cyber threats, the TSA has issued security directives intended for use against specific threat assessment, or threats.

However, those security directives have been referenced as generally disruptive to operations and requiring a great deal of coordinated effort at the implementation point, that takes away from actual monitoring of threat.

There's only so many staff available within the actual entities that operate, say, in our rail and pipelines, and if those men and women that are dedicated, that work in that office, if they have to spend so much of their time and energy complying with the regulatory requirements, then they're not investing that energy into actual monitoring of threats and responding to threats.

So we have a responsibility to attempt to do better. Not that the initial effort was not well-intended, it's just that we're dealing with an emerging and complex threat for the first time in our history.

So Mr. Lorincz and Mr. Gorman, 2 years ago, Congress passed legislation, setting guidelines for reporting cyber attacks at 72 hours. You have to report this within 72 hours, to streamline this in the interest of time.

In TSA's rule, TSA—I'm sorry—72 hours. So—and TSA's rule said, Well, we're going to do it within 24 hours, and the Securities and Exchange Commission finalized rules in 2022, saying it had 4 business days.

So there's a variety of actual implementation responses happening across the Government entities that we must harmonize.

Mr. Chairman, I ask unanimous consent to introduce into the record a media report from November of this year regarding the bipartisan effort to clean up cyber regulations, and to pass legislation that indeed does harmonize our cybersecurity efforts. That would be H.R. 10123.

Mr. GIMENEZ. Without objection.

[The information follows:]

Article Submitted by Honorable Clay Higgins

BIPARTISAN EFFORT TO CLEAN UP CYBER REGULATIONS GETS A BOOST IN HOUSE, BUT CALENDAR IS TIGHT

By Martin Matishak, November 18, 2024, The Record, Recorded Future News

A House Republican late last week introduced legislation to untangle the country's jumble of cybersecurity regulations, keeping the bipartisan proposal alive as Congress finishes its work for 2024.

The measure from Rep. Clay Higgins of Louisiana, a member of both the House Homeland Security and Oversight committees, is a companion bill to bipartisan legislation that sailed through the panel's Senate counterpart in July by a 14–1 vote. Recorded Future News first reported on the proposed law.

Both would require the White House's national cyber director to establish a committee to harmonize the patchwork of cyber requirements imposed on the private sector by Federal regulatory agencies.

The Biden administration has given the legislation its full-throated support, arguing the existing landscape is a myriad of inadequate, and often redundant, requirements that actually harm the nation's digital defenses.

"Duplicative requirements . . . can, perversely, result in worse cybersecurity outcomes, because teams have to focus on compliance instead of directly mitigating cyber risk," Harry Coker, the country's current cyber czar, said at Columbia SIPA cyber conference last week.

But the click is ticking. There are only a few weeks left in the lame-duck session of Congress and there are only a handful of legislative vehicles the regulatory bill—which still has to be approved by committee and then the full chamber—could be attached to. A new Congress starts January 3, and President-elect Donald Trump will take office soon after that, resetting the legislative agenda.

Higgins' legislation could hitch a ride on another short-term government funding bill. The current spending bill expires on December 20. Republicans leaders have already signaled they will punt the issue into 2025 after the GOP secured a trifecta in government by seizing control of the White House and both chambers of Congress.

However, it's possible the proposed regulation overhaul ultimately expires at the end of the current two-year congressional term, meaning proponents would have to try again in the future.

Nicholas Leiserson, assistant national cyber director for cyber policy and programs, held out hope that the legislation would make it through the year-end gauntlet.

"As ever in a lame duck, there's a lot of activity going on at the end of the Congress. But, from our standpoint, this has been a bipartisan issue from the beginning," he told Recorded Future News on Friday during a phone interview.

Leiserson said that "folks from across the political spectrum" have come to support the legislation's goal because it's one of only a "few cases in government where you can actually get better cybersecurity outcomes for less money," noting Auburn University's McCrary Institute last month issued a list dozens of recommendations to revamp Federal cyber policy with harmonizationin the top spot.

Leiserson declined to speculate about what would happen if the bill isn't approved before lawmakers adjourn for the year.

"Our hope is certainly that this is going to get done as soon as possible. That's our priority," he said.

"What happens if it doesn't is really up to the next administration."

Martin Matishak is the senior cybersecurity reporter for The Record. Prior to joining Recorded Future News in 2021, he spent more than 5 years at *Politico,* where he covered digital and national security developments across Capitol Hill, the Pentagon, and the U.S. intelligence community. He previously was a reporter at *The Hill,* National Journal Group and Inside Washington Publishers.

Mr. HIGGINS. Thank you.

Gentlemen, we probably have time if the Chairman would indulge, do you see anything more important, Mr. Lorincz and Mr. Gorman, anything more important than harmonization of our security efforts to protect our Nation's infrastructure from cyber threat?

Mr. GORMAN. TSA supports the overall goal of harmonizing cybersecurity requirements with our industry stakeholders. This is an area specifically where we've asked for feedback, in the NPRM, and based on that feedback, based on other efforts and interagency discussions that are on-going, we anticipate to be able to incorporate that as we move forward into the final rule stage.

Mr. HIGGINS. Thank you.

Mr. Lorincz.

Mr. LORINCZ. Yes, I just wanted to also add to Chad's point, that it's really important for us to make sure that we continue to collaborate with our stakeholders and provide and receive feedback.

To your question and to your comment, I think it's really important to also address, since May 2021, just in the surface realm, we have held over 300 industry engagements, whether it's briefings or calls, to make sure that industry had the opportunity to provide feedback, so we can receive that feedback and pivot accordingly.

Also within the aviation sector, just this year alone, we have had the opportunity to receive feedback from our aviation partners over 126 times, to make sure that we understood and we received the feedback based on their operational needs and necessities.

So we continue to listen because I think it's really, really important to understand that we're on a journey together, and I really, really appreciate the question and the thought about harmonization as we move forward. Thank you.

Mr. HIGGINS. Thank you, sir.

Thank you, Mr. Chairman, for the indulgence.

Mr. GIMENEZ. I thank the gentleman from Louisiana.

I now recognize the gentlewoman from Florida, Ms. Lee.

Ms. LEE. Good morning, and thank you all so much for being here with us today.

Mr. Lorincz, Mr. Gorman, I'd like to start by addressing this question to both of you, and that is, I'm interested in what are some of the critical things, that you identified or addressed through security directives, that TSA is considering as part of the formal regulatory process?

Mr. GORMAN. I think the most important lesson that we learned collectively with our industry stakeholders in the issuance and the performance of the requirements within our current security directives, is that there is no one-size-fits-all when it comes to cybersecurity, particularly when it comes to the complexity of the threat and the complexity of business and operational technology networks in place today.

So, we believe and have learned the lesson through the issuance and the maintenance of those requirements in the SDs, and in moving those into this proposed rule, that a performance-based model is the only way that we will be successful, and our partners will be successful in continuing to prevent disruptive attacks against our Nation's transportation infrastructure.

We believe that as you look at the requirements of this rule set, those—that theme has carried over, but particularly, we are interested in industry feedback as it relates to both the opportunities that it provides them to customize these performance-based requirements for their own business operations, as well as potential challenges that they see and how we can incorporate that into the final rule.

Ms. LEE. Tell me, if you would, how that performance-based model accommodates the different sectors that you are attempting to regulate?

Mr. GORMAN. So I believe, again, in the same model is that we establish outcome-based goals across our requirements that are based, again, in industry standards. Like we see in NIST's Cybersecurity Framework, the Cyber and Infrastructure Security Agency's performance-based cyber goals have given those as the platform.

Given the model that we have put in place and are seeing results already of in the SDs, we then work with individual owners and operators to craft specific implementation plans for those measures that are specific to their industry, their technologies, their operations, and the size and scope of those operations, and the technologies, both from a business and from an operational technology perspective that they operate.

Then based on that and based on an assessment of criticality, they then propose to TSA a time line of investments and actions to drive toward those requirements, and we have seen early successes in that model and anticipate continuing that as we move into the final rule.

Ms. LEE. So is it your assessment that that is a sufficient way to identify regulatory requirements that are unique enough for each of the different sectors, that that is a sufficient way to accommodate the notion that each of them needs something a little bit different, and the best practices and requirements for each of those different sub sectors should be a little bit different? You think that's an adequate way to address it?

Mr. GORMAN. I think not only do we believe it's adequate, we believe that is one, again, an essential way to provide the flexibility across infrastructure, as well as provide flexibility for continuing adapting in persistent threat environment. So as we, again, move into a permanent rule stage, we believe that is the way that we will provide and actually work with our partners for ultimate success.

Ms. LEE. Mr. Lorincz, anything to add on that subject?

Mr. LORINCZ. Yes, thank you. I think to the points that were made earlier, I think for us, the relationship building is really, really critical, understanding industry, and to the previous answer that one size does not fit every one of those entities, making sure that they're able to work together.

One thing that's really, really important to mention is that as they build those plans, those plans are built with us. We help them through that journey.

It's also important to note before we send out any teams to do any inspections or assessments, we have conversations that take place weeks before to make sure that they're ready. This is not a gotcha mentality.

This is all about making sure that we keep the system safe. So we spend a lot of time investing, making sure that at the end, we have a great product and that product is safe. If there's anything that we need to do to pivot, to make sure that we're able to adjust, that we do that accordingly.

Ms. LEE. Is TSA adequately resourced to implement what the proposed rules require?

Mr. LORINCZ. So we are very—we appreciate the support that we have received, as I stated earlier, and we look forward to receiving the additional 41 assets that is in the fiscal year 2025 President's budget.

Ms. LEE. Mr. Chairman, I yield back.

Mr. GIMENEZ. Thank you to the gentlewoman from Florida.

I want to thank the witnesses, Mr. Lorincz, Mr. Gorman, and Dr. Sherman, for your valuable testimony, and the Members for their questions. The witnesses are now dismissed, and the committee will stand in brief recess—very brief recess—while the clerk shall arrange for the second panel of witnesses.

[Recess.]

Mr. GIMENEZ. The committee will come to order. I am pleased to welcome our second panel of witnesses. I ask that the witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. GIMENEZ. Let the record reflect that the witnesses have answered in the affirmative, thank you, and please be seated.

I would now like to formally introduce our second panel of witnesses. Mr. Ian Jefferies serves as the president and chief executive officer of the Association of American Railroads.

Ms. Kimberly Denbow serves as the vice president of security and operations for the American Gas Association.

I thank each of our distinguished witnesses for being here today. I now recognize Mr. Jefferies for 5 minutes to summarize his opening statements.

STATEMENT OF IAN JEFFERIES, PRESIDENT & CHIEF EXECUTIVE OFFICER, ASSOCIATION OF AMERICAN RAILROADS

Mr. JEFFERIES. Good morning, Chairman Gimenez, Members of the subcommittee. Thank you for the opportunity to be here today where I have the privilege of representing the Nation's freight railroads.

Running across 140,000 miles of privately-funded infrastructure, railroads rely on advance technology and skilled employees to operate safely and keep goods moving every day.

Safety, physical and digital, is at the core of all railroads do, and pertaining to cybersecurity specifically, as you know, it is a continuous arms race between attackers and defenders, with railroads committed to constantly improving protection.

If you take away one thing from me today, I hope it is this: Railroads have a track record and a system in place to meet the cyber challenges of today and tomorrow.

We prioritize cybersecurity through a well-established, risk-based, and collaborative approach, actively working with Government entities like TSA and CISA to improve and adapt cybersecurity measures.

This includes regularly-scheduled interaction between industry and our Government partners, where both threats and preparedness levels are analyzed in depth.

Moreover, railroads have a long-standing commitment to protecting their operations through coordinated efforts and continuous evaluation of cybersecurity plans.

Our unified security plan evolves with input from private and Government experts to address emerging threats effectively.

With that, let me turn to some details. As I mentioned, railroads emphasize information sharing with agencies like TSA and CISA to stay ahead of threats.

Rail industry leadership has played a central role as well, starting with the establishment of a unified cybersecurity plan over 20 years ago.

Cybersecurity plans are implemented by two bodies—the Rail Security Working Committee, which focuses on countering terrorism, and the Rail Information Security Committee, composed of information security leaders from major railroads. Together these committees form the Rail Sector Coordinating Council, railroads' main channel for coordinating with Government on cybersecurity.

Looking forward, while railroads and other entities have been reporting incidents for several years, railroads would benefit from CISA regularly updating its cyber profile based on attack analyses across sectors, as timely reports back to industry are crucial for staying informed about emerging threats and potential bad actors.

In looking at the risk management rule, AAR appreciates the open regulatory approach TSA has finally taken with regard to its recent NPRM on cyber risk management. The industry is still reviewing the rule, which just came out this month and will offer detailed comments.

In our initial review of the NPRM, we did identify a few long-standing issues railroads have repeatedly raised with TSA that were not addressed in the NPRM.

For example, and as mentioned earlier, the proposed rule requires the reporting of a cyber incident in 24 hours, which conflicts with the statute requirement of 72 hours, further conflicting with the SEC requirements of 4 days.

Not only could this conflict create confusion, and was easily avoidable, but the earlier deadline may divert resources from immediate on-going attack response to comply with the reporting requirement.

The rule also continues to require that any security coordinator be a U.S. citizen which is impossible for a Canadian class I railroad to operate throughout the United States as well.

We look forward to addressing these issues and others throughout the public comment period and will continue to engage in conversations with TSA and other Government partners to ensure any final rule protects railroads, employees, and the communities in which we operate.

As I said, we were pleased to see TSA issue this proposed rule through a normal regulatory process after several years of issuing security directives under its emergency authorities.

While emergency authorities might be necessary in the rare instance of a true, identical immediate threat, AAR prefers the collaborative regulation over TSA's use of directives, which, while faster, bypass public input and risk leading to unnecessary requirements that lack security justification.

One-size-fits-all prescriptive mandates can be counterproductive by failing to recognize the modal differences in their cyber preparedness. As I mentioned, railroads' first cybersecurity plan was established over 20 years ago.

Overly prescriptive regulation also risks stifling innovation necessary to adapt to constantly-changing threats, something that is happening every day.

AAR supports performance-based standards—and that was a welcome message from the prior panel—to allow flexibility in responding to fast-evolving threats.

Thank you, and I look forward to our discussion today.

[The prepared statement of Mr. Jefferies follows:]

Prepared Statement of Ian Jefferies

November 19, 2024

INTRODUCTION

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to testify on how the rail industry works with our Government counterparts to address cyber threats and the impacts of emergency authority on those efforts. AAR's members account for the vast majority of North American freight railroad mileage, employees, and traffic.

Freight railroads integrate skilled personnel and ingenuity with technology to keep the network infrastructure safe and the supply chain moving every day. Advanced information and communications technology are helping our employees in every aspect of our operations, including train control, track and equipment inspections, emergency response, dispatching, railcar tracking, locomotive fuel management, predictive performance analysis, employee training, and much more. Cybersecurity is an arms race between attackers and defenders, which is why our highly-skilled, highly-trained employees work diligently to continually enhance their capabilities and guard against cyber attacks that threaten the safety and integrity of our operations.

For 25 years, railroads have maintained a dedicated coordinating committee focused on cyber threats, effective risk mitigation practices, and engagement with appropriate Government entities. Railroads leverage a strong mix of private and public capabilities to effectively prevent and respond to malicious cyber activity. As threats evolve, our industry strives to stay agile and innovative to address the dynamic threat landscape.

A UNIFIED COMMITMENT TO OVERALL SECURITY PREPAREDNESS

The rail industry addresses cybersecurity head-on through a long-standing industry-wide, risk-based, and intelligence-driven plan. Railroads' highly specialized cybersecurity teams carry out comprehensive, multi-faceted cybersecurity plans focused on 4 factors identified by experts as the most likely way to stop cyber attacks: the tactics most commonly used to gain illicit access to computer systems; the vulnerabilities most commonly exploited; illicit activities missed or disregarded in prior analysis but identified after the incident; and protective measures that could have made a difference had they been implemented.

Responsibility for implementing and sustaining cybersecurity plans lies with two specialized industry coordinating bodies. First, the Rail Security Working Committee includes senior law enforcement and security officials focused on countering domestic and international terrorism. Second, the Rail Information Security Committee (RISC) is comprised of chief information security officers and information assurance leaders from major North American railroads. The RISC was established in 1999 and is supported by security experts from the AAR and the American Short Line and Regional Railroad Association (ASLRRA). Together, these committees form the Rail Sector Coordinating Council (RSCC), the rail industry's primary channel for communication and coordination with Government agencies on cybersecurity initiatives.

The rail industry's security plan does not just sit on a shelf. It is a living document, continuously evaluated and enhanced through recurring exercises and frequent consultations with Government and private-sector security experts to ensure maximum sustained effectiveness supported by a strong working relationship with the Federal Government.

INFORMATION SHARING IS VITAL FOR SUCCESS

For railroads, cyber awareness is a fundamental component of their day-to-day operations, but even the best cybersecurity plans and practices will falter if useful information on cyber threats is not shared. Information sharing allows organizations to learn from one another, reduce their vulnerabilities, and quickly adapt to changing conditions. Insights gained from risk assessments and threat advisories, along with experience gained in drills, enable railroads and industry organizations to incorporate effective safeguards and protective measures into their own systems.

For this reason, railroads and industry organizations prioritize proactive engagement with Government partners, including the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA), to share information on cyber threats and effective countermeasures. These open lines of communication are maintained through frequent calls and meetings between AAR, its members, and TSA, ensuring our Federal Government partners are aware of how rail operations interact with cybersecurity measures.

NOTICED OF PROPOSED RULEMAKING (NPRM)

Earlier this month, TSA issued a lengthy NPRM that builds upon existing cybersecurity requirements previously issued through security directives. While the industry was pleased to see TSA issue this rule through the regulatory process and allow for robust public comment, the NPRM would have greatly benefited from earlier discussions with industry about potential requirements in a more informal setting like negotiated rule making. The industry is still digesting the very lengthy proposal and will provide robust comments. There are a few long-standing concerns for the railroads that the NPRM does not fully address.

For example, the NPRM would require railroads to report an incident within 24 hours of it occurring. Congress specifically set the time frame for reporting incidents at 72 hours under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Not only does this lack of harmonization create confusion, the 24-hour window is impractical. Within 24 hours, an attack could still be occurring, the information about the incident will be less complete, if not inaccurate, and railroads would be pulling resources and manpower away from responding to the attack and toward complying with reporting requirements. The railroads would have to then supplement the initial report as their information becomes available or changes.

Similarly, the NPRM also requires that a railroad's security coordinator be a U.S. citizen, which the railroads have flagged with TSA as a major concern for several years. Two large railroads in the United States are headquartered in Canada and employ Canadian citizens in high-level cybersecurity roles. Prohibiting these highly-skilled senior-level employees from representing their companies as security coordinators serves no clear security benefit and makes it extremely difficult for these Canadian railroads to comply.

USE OF TSA EMERGENCY AUTHORITY

AAR was pleased that TSA finally issued this NPRM. For several years, the industry was operating under security directives issued under TSA's emergency authority. We recognize the importance of TSA having the appropriate authority to act quickly in the face of an emergency. However, following the Colonial Pipeline attack in 2021, TSA used its emergency authority to issue security directives aimed at freight railroads and other modes of critical infrastructure mandating specific requirements effective immediately. AAR was unaware of, nor was it made aware of, any prevailing freight rail emergency conditions that would require use of emergency authority, and the security directives circumvented the notice and comment period that allows for industry feedback to improve regulations. The broad mandates TSA issued also treated every mode as if they were starting from scratch with developing a cybersecurity plan when railroads had been properly monitoring their network for decades. The decision by TSA to issue the recent NPRM and move away from security directives and toward the normal rule-making process is a welcome one that will make these regulations more effective.

OTHER AREAS FOR IMPROVEMENT

AAR has identified 2 other areas where our work with TSA and other agencies could be improved. First, the lack of analysis of cyber incidents by the Government can leave railroads and other modes unaware of future threats or how to reduce susceptibility to future attacks. Further analysis of an attack or other incidents by the Government can inform railroads' decisions about strengthening our network. Second, the Government's focus on the cybersecurity risks of transportation companies overlooks the importance of ensuring the security of suppliers to the industry. Suppliers play a critical role in various aspects of railroad operations, and the Government should consider how best to directly address their vulnerability to cyber incidents.

CONCLUSION

The railroad industry, TSA, and CISA share a common purpose: ensuring that effective, up-to-date, and sustainable measures are in place to mitigate risk in the face of evolving cyber threats. Railroads have a proven track record of cooperative engagement with Federal agencies, and they firmly believe that collaborative effort is the best way to achieve this goal. Railroad operations are resilient thanks to years of proactive and extensive efforts by highly-skilled railroad employees to develop, implement, and continuously improve plans, practices, and measures for cybersecurity as threats and security concerns emerge. Cybersecurity is always evolving, and real-time adaptation is essential to reduce risk. Railroads and their employees will continue to work cooperatively with private and public entities to ensure that our Nation's rail network and the people, firms, and communities we serve remain safe, efficient, and secure.

Mr. GIMENEZ. Thank you, Mr. Jefferies.

I now recognize Ms. Denbow—Denbow or Denbow?

Ms. DENBOW. Denbow, sir.

Mr. GIMENEZ [continuing]. For 5 minutes to summarize her opening statements.

STATEMENT OF KIMBERLY DENBOW, VICE PRESIDENT, SECURITY OPERATIONS, AMERICAN GAS ASSOCIATION

Ms. DENBOW. Thank you, Chairman. Chairman Gimenez, Members of the subcommittee, I am Kimberly Denbow, vice president of security and operations of the American Gas Association, AGA.

AGA represents more than 200 local energy companies that deliver clean and affordable natural gas to 95 percent of natural gas customers across the United States.

I have led AGA security policy and technical program for nearly 3 decades. I'm a former voting member of the TSA Surface Transportation Security Advisory Committee and co-chaired the standing-up of its cyber subcommittee.

Thank you for inviting me to this hearing to share our experiences as they relate to how TSA puts its regulatory authority into practice.

America's natural gas utilities and TSA share a common mission—critical infrastructure and operator security.

For over 2 decades, TSA and natural gas utilities have challenged the traditional regulatory model, piloting forward-leaning approaches to achieve a common mission, to achieve our common mission—critical infrastructure and operator security.

While TSA has full authority to regulate pipeline security, it boldly opted for an unconventional and more effective model TSA coins as structured oversight.

TSA recognized early on the strength in the pipeline sector's operational diversity and that system disruptions and consequences differ substantially across the natural gas and oil value chains.

While the Colonial Pipeline ransomware incident in 2021 propelled TSA into regulating pipeline cybersecurity, TSA and owner-operators had been weighing the importance of pipeline cybersecurity well before 2021.

Over the decade following the 2012 Chinese cybersecurity campaign that targeted pipelines, TSA and pipeline owner-operators worked collaboratively to advance pipeline cybersecurity maturity.

Beyond basic cybersecurity hygiene, TSA realized there is no single cybersecurity law, regulation, or standard that can be universally applied across pipelines without having to allow the option of alternative measures or system-by-system customization.

Regardless, public pressure in the aftermath of the Colonial Pipeline ransomware incident drove TSA to issue a series of prescriptive, emergency security directives covering pipeline cybersecurity.

The first iteration of security directives was depicted by inapplicable cybersecurity measures and unattainable compliance time lines.

AGA worked tirelessly educating TSA about the operators' concerns. TSA ultimately hosted a series of pipeline security directive technical roundtables, and listened and learned directly from owners and operators about alternative and in many cases, more effective approaches to achieving the same cybersecurity outcome as required by the prescriptive measures.

The technical roundtables resulted in a major regulatory course correction of the security directives toward a risk-based, outcome-focused approach.

Let's get real. A proactively informed regulator is less likely to promulgate unclear, misinformed, and unworkable regulations.

We recognize security directives serve a logical purpose. Imminent threats require immediate action.

As demonstrated by the technical roundtables and subsequent TSA-hosted forums, there are benefits from leveraging security directives to improve security requirements before embedded into final rules.

There must be a balance, however, because each iteration of the pipeline security directives results in reallocation of security resources on the part of the owner-operator.

Congress should place guardrails on this regulatory mechanism to reduce its potential for future abuse or misuse.

Hallelujah. After 4 years of being regulated by security directives, TSA finally issued cybersecurity regulations—proposed cybersecurity regulations.

AGA member utilities favor reasonable pipeline cybersecurity regulations that are attainable, sustainable, and auditable, and we applaud TSA for sticking with a risk-based, outcome-focused approach.

We look forward to submitting constructive comments intended to advance TSA's and AGA-member, natural gas utilities' common mission.

I would like to add—and I think that this is very important to spotlight—I want to spotlight unresolved concern that applies to the pipeline security directives, to the TSA cybersecurity rule making, and appears to be a systemic problem across the Government—the fixation on collecting and aggregating security operations-related sensitive information of critical infrastructure.

There lacks rhyme and reason as to why any Government entity in this threat environment would be compelled to take possession of critical infrastructure's most sensitive, security operations-related information.

It's ironic the onus is on the owner and operator to limit the vulnerabilities introduced by sub-par Government cybersecurity performance, which continues to play itself out incident after incident. This is the one area where the Government continues to fail in our common mission.

Thank you for the opportunity to testify. I look forward to the exchange.

[The prepared statement of Ms. Denbow follows:]

Prepared Statement of Kimberly Denbow

November 19, 2024

Chairman Gimenez, Ranking Member Thanedar, and Members of the subcommittee, I am Kimberly Denbow, vice president of security and operations, at the American Gas Association (AGA). I have led AGA's security policy and technical program for nearly 3 decades. I am a former voting member of the Transportation Security Administration (TSA) Surface Transportation Security Advisory Committee and helped stand up and co-chaired the Cybersecurity Subcommittee. I also stood up and presently co-chair the Cybersecurity Working Group of the Oil & Natural Gas Subsector Coordinating Council. Additionally, I have worked with TSA and its pipeline security section since TSA's inception. Thank you for inviting me to share my perspectives on the natural gas utility experience with TSA, specifically as they relate to how TSA puts its regulatory authority into practice.

AGA, founded in 1918, represents more than 200 local energy companies that deliver clean, domestic, and reliable natural gas throughout the United States. There are more than 78 million residential, commercial, and industrial natural gas customers in the United States, of which 95%—more than 74 million customers—receive their gas from AGA members. Today, natural gas meets more than one-third of our Nation's energy needs. AGA members recognize that with the benefits and opportunities natural gas offers our country, there comes great responsibility to protect our distribution pipeline system network from cyber compromise.

AGA members have been at the forefront of cybersecurity investment and are continually seeking ways to improve their cybersecurity readiness. The AGA board of directors passed a resolution in 2021 in favor of reasonable cybersecurity regulations, and AGA and its members engage in every opportunity to work with Federal Government partners and regulators to promote risk-based cybersecurity programs that support security measures that are attainable, sustainable, and auditable. This includes extensive work with TSA to help strengthen and add value to the pipeline Security Directives (SDs)[1] and reduce risk for the industry. Risk-based cybersecurity aligns with the National Security Memorandum on Critical Infrastructure Security and Resilience.[2]

Technological advances continue to make natural gas operations safer, more cost-effective, and better able to serve customers via web-based programs and tools. The corollary to a more connected and more efficient industry is our attractiveness as a target for increasingly sophisticated nefarious cyber actors. This said, America's natural gas utilities are combatting the threat daily via:

- Skilled personnel,
- Robust cybersecurity system protections,
- Industry commitment to security,
- Collaboration with other industries and associations,
- On-going cybersecurity partnerships with the Federal Government, and
- Interaction with the Downstream Natural Gas Information Sharing & Analysis Center (DNG–ISAC) Community for real-time awareness and action.

[1] Security Directive Pipeline 2021–01, issued May 26, 2021: *Enhancing Pipeline Cybersecurity* (SD1), and Security Directive Pipeline 2021–02, issued July 19, 2021: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (SD2). The SD's have been reissued annually since 2021. Per TSA Administrator David Pekoske, the SDs will continue to be reissued until cybersecurity regulations are promulgated.

[2] National Security Memorandum on Critical Infrastructure Security and Resilience, The White House, (April 30, 2024), available at *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/* (last visited November 15, 2024).

A COMMON MISSION—PROTECTING AMERICA'S NATURAL GAS UTILITIES

AGA and its member companies are committed to utilizing leading security practices and training, investing in purposeful security technologies, and promoting an industry-wide vigilant security culture to fortify our security defenses and enhance all aspects of safety. TSA's mission is to "Protect the nation's transportation systems to ensure the freedom of movement of people and commerce".[3] To that end, America's natural gas utilities and TSA share a common mission—critical infrastructure and operator security.

In a cojoined journey over 2 decades, TSA and natural gas utilities have challenged the traditional prescriptive regulatory model, piloting unconventional approaches to achieve this common mission. All parties acknowledge that "check-the-box" compliance does not equate to security, and that numerous paths can lead to the same security outcome. The following provides an overview of AGA and AGA-member natural gas utility experience with TSA in its role as the Federal pipeline security regulator but also as a model of functional public/private partnership.

STRUCTURED OVERSIGHT

TSA was created in the aftermath of 9/11 to oversee the security of multiple transportation modes including commercial and general aviation, mass transit systems, freight and passenger rail, and highways, pipelines and ports.[4] TSA became part of the Department of Homeland Security in March 2003 and organizationally consists of 2 primary divisions, aviation and surface transportation.

The general public associates TSA with airport security, and historically, the majority of transportation security funding goes to aviation security. Secondary to aviation, TSA regulates security operations for the 4 surface transportation modes—mass transit, freight rail, highway motor carrier, and pipeline.

TSA's first decade of surface transportation security operations was organized by mode. For example, TSA operated a Pipeline Security Branch, staffed by subject-matter experts, who understood the complexities of pipeline commerce (e.g., transporting liquids differs from transporting natural gas) and collaborated with pipeline owners/operators to learn the security nuances of individual pipeline systems. While this branch of TSA had full authority to regulate pipeline security, it opted for an unconventional and more effective non-regulatory, collaborative model TSA coined as "structured oversight." TSA chose this methodology in part because a one-size-fits-all regulatory approach was inappropriate given operational variations between the natural gas and liquid hydrocarbons (e.g., oil) value chains. While the structured oversight approach is resource-intensive for TSA to effectively prepare, conduct, and follow up on security inspections (as well as track security threats), this collaborative method represents a common public-private mission, benefits both the regulator and regulated entity, and advances pipeline sector security.

This organizational structure changed in the 2012/2013 time frame. TSA eliminated dedicated modal branch security operations for each surface transportation sector in favor of a multi-modal oversight system where TSA surface transportation staff may or may not have specific expertise necessary to evaluate the infrastructure they were assigned. The Pipeline Security Branch's full-time equivalents (FTEs) were reduced by 93% (from 14 down to 1).[5] AGA publicly expressed concern about replacing TSA pipeline subject-matter experts with generalists. Nevertheless, and despite this ill-advised decision, the collaboration between TSA and pipeline owners/operators did not wane.

Over time at industry's urging, TSA has steadily rebuilt pipeline security capability and personnel. For example, TSA Administrator David Pekoske's testimony before the U.S. Senate Committee on Commerce, Science, and Transportation on July 27, 2021, notes that passage of the TSA Modernization Act allowed TSA to" . . . expand pipeline security staff to 39 FTEs working in field operations, headquarters operations, and policy development . . . [and] trained a 20-member field-based Pipeline Security Assessment Team (PSAT) . . . ".[6] Today, TSA con-

[3] TSA's Mission Statement, TSA, available at *https://www.tsa.gov/about/tsa-mission* (last visited November 15, 2024).

[4] TSA at a Glance Factsheet, TSA, available at *https://www.tsa.gov/news/press/factsheets/tsa-glance-factsheet* (last visited November 15, 2024).

[5] *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management,* GAO, (Dec. 18, 2018), available at *https://www.gao.gov/products/gao-19-48* (last visited November 15, 2024).

[6] Pipeline Cybersecurity: Protecting Critical Infrastructure, TSA, (July 7, 2021), available at *https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure* (last visited November 15, 2024).

tinues to collaborate with owners/operators to learn about their pipeline systems and improve methods to secure pipeline infrastructure overall.

TSA Pipeline Security Guidelines

The TSA Pipeline Security Guidelines (Guidelines)[7] are the heart of the structured oversight model and serve as a foundation upon which pipeline owners/operators have built their security programs for the last 2 decades. The Guidelines were developed and updated in tandem with pipeline owners/operators and Government cohorts, including the Pipeline & Hazardous Materials Administration, the Department of Energy, the Department of Homeland Security (DHS), and the Federal Energy Regulatory Commission (FERC). While adoption of the Guidelines is voluntary, TSA maintains the authority to regulate as necessary.

The first edition of the Guidelines in 2010 mainly focused on physical security (given the events of 9/11) rather than cybersecurity. Following the targeted Chinese cybersecurity campaign[8] against pipelines in 2013, the Guidelines were revised to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[9]

Implementing the Guidelines prepares pipeline owners/operators for TSA on-site Corporate Security Reviews (CSR) and Critical Facility Security Reviews (CFSR). CSRs assess the degree to which the Guidelines' physical and cybersecurity measures are integrated into the operator's corporate security plan. CFSRs are conducted at critical pipeline facilities to collect site-specific information on facility security policies, procedures, and physical security measures.[10] Overall, CSRs and CFSRs have historically focused more on physical security and are intended to serve as an opportunity for TSA to work collaboratively with owners/operators to advance security, in notable contrast to an adversarial standard regulatory compliance methodology.

As TSA develops cybersecurity capabilities, AGA encourages TSA to also maintain its attention on physical security. For example, a widely-used TSA resource, the Pipeline Security Smart Practices,[11] is a compilation of valuable physical security practices observed from CSRs and CFSRs. For a few years, TSA did not update the resource due to directing full attention to the SDs. Regularly adding to this resource assists those owners/operators that have not yet undergone a CSR or CFSR.

Additionally, from a threat perspective, TSA continues to miss the mark in characterizing the physical security threat level to domestic pipelines. Despite owners/operators reporting increasing incidences of pipeline sabotage activity, including malicious vandalism, intentional damage to pipeline infrastructure, trespassing and unauthorized operation of pipeline valves and other equipment, finding improvised explosive devices on pipeline infrastructure, and assaults on pipeline operators and contractors, TSA consistently presents the physical security threat level as low. It is our understanding that this threat level assessment is not sourced from within TSA. Regardless, it is incumbent on TSA to reconcile the discrepancy between what the Federal Government intelligence community is observing and what the pipeline owners/operators are experiencing. The Federal Government's mischaracterization of the pipeline physical security threat level not only threatens pipeline security readiness, it also negatively impacts gas utility security investment. Natural gas utilities are State-regulated via public utility commissions (PUCs), which oversee customer rates and utility expenses and investments. The more TSA continues to underestimate pipeline security threats, the more difficult it is for natural gas utility owners/operators to justify pipeline security investments to State PUCs.

Growing Cybersecurity Capabilities

While the Colonial Pipeline ransomware incident in 2021 propelled TSA into regulating pipeline cybersecurity, TSA considered the importance of pipeline cybersecurity well before 2021. The Chinese cyber campaign targeting pipelines that surfaced

[7] Pipeline Security Guidelines, TSA, (March 2018), available at *https://www.tsa.gov/sites/default/files/pipeline__security__guidelines.pdf* (last visited November 15, 2024).

[8] Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013, CISA, (July 2021), available at *https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a* (last visited November 15, 2024).

[9] Cybersecurity Framework/NIST (last visited November 15, 2024).

[10] Pipeline Cybersecurity: Protecting Critical Infrastructure, TSA, available at *https://www.tsa.gov/news/press/testimony/2021/07/27/pipeline-cybersecurity-protecting-critical-infrastructure#:?:text=Working%20with%20pipeline%20operators%27%20'security,the%20operator%27s%20corporate%20'security%20plan.* (last visited November 15, 2024).

[11] Pipeline Security Smart Practice Observations, TSA, (September 19, 2011), available at *https://www.tsa.gov/sites/default/files/tsapipelinesecuritysmartpracticeobservations__2011-__508.pdf* (last visited November 15, 2024).

in 2012[12] led to a cybersecurity paradigm shift across the pipeline industry and TSA. Over the decade that followed, TSA and pipeline owners/operators worked collaboratively on:

- Applying existing Federal Government-developed cyber assessments tools,
- Developing a pipeline-specific cyber assessment,
- Conducting DHS Validated Architectural Design Reviews,[13]
- Updating the cyber section of the Pipeline Security Guidelines to align with the NIST Cyber Security Framework,[14] and
- Developing API 1164 3d edition, Pipeline Control Systems Cybersecurity,[15] a consensus-based standard worked on by owners/operators, vendors, and Federal Government representatives (including TSA and FERC).

By that time, TSA had worked with pipeline owners/operators long enough to recognize that there is strength in operational diversity and that system disruptions and consequences will differ substantially across the natural gas and oil value chains—and further within the different segments of each value chain (e.g., natural gas utility, natural gas transmission, LNG operations). Beyond basic cybersecurity hygiene, there is no single cybersecurity law, regulation, or standard that can be universally applied across pipelines and LNG operations without having to allow the option of alternative measures or system-by-system customization. TSA further recognized it needed to build up its internal cybersecurity expertise despite minimal funding available for pipeline security, let alone for pipeline cybersecurity.

Despite this concerted effort by TSA to thoughtfully approach the development of cybersecurity regulations for the broader pipeline industry, public pressure in the aftermath of the Colonial Pipeline ransomware incident drove TSA to immediately issue a series of prescriptive emergency Security Directives (SDs) covering pipeline cybersecurity. The initial SDs were filled with unattainable cybersecurity measures and compliance time lines that, rather than improving sector cybersecurity, actually increased pipeline system vulnerability and threatened system reliability. The first iteration of pipeline cyber SDs was a textbook case study of what a regulator should not do.

TSA AS CYBERSECURITY REGULATOR

Pipeline Security Directives—An Informed Regulator

The first iteration of SDs, specifically the Security Directive Pipeline–2021–02 series (known as SD2[16]), was unreasonably prescriptive, without regard for pipeline owners/operators cybersecurity system applicability, operational feasibility, and compliance time lines. They were issued as a one-size-fits-all, prescriptive cybersecurity measures to TSA-designated critical oil and natural gas pipeline systems. AGA worked tirelessly with every level of TSA to draw attention to the impracticality, ineffectiveness, and financial irresponsibility of these prescriptive measures, which would have resulted in minimally improved security, but at the expense of increased cybersecurity vulnerability in many pipeline systems.

Reflecting 2 decades of genuine collaboration between TSA and pipeline owners/operators, TSA ultimately agreed to host Pipeline Security Directive (PSD) Technical Roundtables (Technical Roundtables) on SD2 to hear directly from owners/operators about how these mandated cybersecurity measures were unattainable, and that there were alternative and more effective approaches TSA should consider. "On July 21, 2022, TSA issued Security Directive Pipeline–2021–02C, transitioning the requirements of the previous versions in the [SD2] series to be more performance-based and less prescriptive. The performance-based approach enhanced security by mandating that critical security outcomes are achieved while allowing owners/operators to choose the most appropriate security measures for their specific systems and operations."[17] Bottom line, the TSA Technical Roundtables resulted in a major regu-

[12] Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013, CISA (July 21, 2021), available at *https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-201a* (last visited November 15, 2024).

[13] Validated Architecture Design Reviews (VADR) Sample Report, CISA, (December 17, 2020), available at *https://www.cisa.gov/resources-tools/resources/validated-architecture-design-review-vadr-sample-report* (last visited November 17, 2024).

[14] Cybersecurity Framework, NIST, available at *https://www.nist.gov/cyberframework* (last visited November 17, 2024).

[15] API Standard 1164, 3d Edition, API, (August 2021) available at *https://www.api.org/products-and-services/standards/important-standards-announcements/1164* (last visited November 17, 2024).

[16] Security Directive Pipeline 2021–02, issued July 19, 2021: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing (SD2). The SD2 is labeled Sensitive Security Information.

[17] Federal Register: Ratification of Security Directives (last visited November 17, 2024).

latory course correction that eliminated prescriptive and unworkable cybersecurity requirements in favor of an almost entirely performance-based and outcome-focused regulation. The credibility established between TSA and owners/operators prior to the Colonial Pipeline ransomware incident and reinforced through Technical Roundtables continues to inform improvements to subsequent iterations of the SDs. Particularly noteworthy, TSA's Surface Operations leadership regularly hosts forums to garner feedback from owners/operators regarding ways to strengthen SD implementation and owners/operator compliance.

The pipeline sector has now complied with nearly 4 years of emergency TSA SDs, and it is highly possible the SDs will be extended into a fifth year or longer. With each iteration, there is a refinement of components in the expiring SD. This is positive. Not so positive is the addition of cybersecurity technical mandates in each new iteration that are inapplicable, confusing, extremely costly, and disruptive to owners/operators, who must substantially alter their compliance procedures from those required by a previous version of the SD. TSA can avoid this ineffectiveness by conducting regular Technical Roundtables in advance of each future iteration. Proactive Technical Roundtables offer owners/operators the chance to clarify new regulatory definitions, requirements, and compliance measures as well as limit potential misinterpretations by TSA and pipeline owners/operators. A proactively-informed regulator is less likely to promulgate unclear, misinformed, and unworkable regulations.

SD Governance—While Purposeful, Needs Guardrails

SDs serve a logical purpose—imminent threats require immediate action. That said, long-term compliance with multiple iterations of SDs over multiple years raises due process concerns because, unlike the standard regulatory process, regulated entities have minimal official input into how SDs are developed and enforced. While there is benefit with leveraging SDs to improve on regulatory requirements before the mandates are embedded into final rules, each iteration of the current SDs has resulted in reallocation of industry resources. This constant pivoting for the sake of regulatory compliance distracts from an owners/operators risk reduction efforts, and it makes securing resources (e.g., such as qualified labor force) difficult.

Furthermore, regulating by SD is at odds with how natural gas utilities operate. SDs, by design, do not allow long-term planning. In contrast, natural gas utilities necessarily rely on multi-year capital budgeting and infrastructure investments. Even nominal increases in annual costs can be extremely challenging. Internally, well-planned cybersecurity plans must be reprioritized if the owners/operators must wait for TSA to "approve" changes in cyber plans and assigned personnel. Externally, State PUCs maintain regulatory oversight over natural gas utility expenses and require owners/operators to have clearly-defined plans for implementation, sustainability, and benefit to the gas utility customer.

Finally, SDs have a different governance framework than traditional rule makings. SDs can be issued by the TSA administrator in response to an imminent threat without due process procedures and activities, such as public comment or economic burden analysis. SDs expire after 12 months, at which time they can be reissued. While recognizing that TSA should maintain some reasonable emergency authority to issue SDs, Congress should consider placing guardrails and time limits on this regulatory mechanism to reduce its potential to be abused or misused.

Rule Making

In late 2022, following the extension of the original SDs into a second year, TSA issued an Advanced Notice of Proposed Rulemaking. AGA member utilities supported this action, favoring reasonable pipeline cybersecurity regulations provided they are attainable, sustainable, and auditable by TSA. As 2023 progressed, pipeline owners/operators urged TSA to proceed with a pipeline cybersecurity rule making rather than continuing to regulate by SDs. The Notice of Proposed Rulemaking for this, now multi-modal, rule was not released until November 7, 2024. Had TSA moved a pipeline-only cybersecurity rule making, the whole process would have likely concluded a year ago. While we understand TSA's interest in consolidating 3 surface modes into a single rule making, this has unnecessarily prolonged the SD process for pipelines. Bottom line, we recognize the urgency that drives the issuance of SDs, however, there need to be guardrails to limit the "regulating-by-SD" approach so that Government and the affected industry can quickly and appropriately move toward a standard regulatory process.

Relative to the recently-released NPRM, AGA commends TSA for issuing proposed rules that are risk-based, outcome-focused, and for the most part, an extension of the recent iterations of the pipeline SDs. That said, 2 areas within the NPRM, corporate cybersecurity governance responsibilities and supply chain cybersecurity integrity are prescriptive, confusing, and in some cases unachievable and were never covered in TSA's previous pipeline SDs. A third area, employee cyber training, was introduced in the most recent SD, but is fully and unhelpfully prescriptive in the NPRM. These unexpected regulatory roadblocks could have been circumvented had TSA hosted Pipeline Security Technical Roundtables (similar in structure to the Pipeline Security Directive Technical Roundtables) before drafting the proposed regulation. TSA missed opportunities to gain useful owners/operator insight and avoid stakeholder confusion.

Federal Government Possession of Owners/Operators Sensitive Operational Information

While the Federal Government is driving itself to a zero trust[18] approach, TSA's NPRM proposes to collect and aggregate security and operations-related sensitive information of critical infrastructure; thus, preventing those owners/operators from achieving the same zero trust environment the Federal Government has been directed to achieve. Many entities in the Federal Government have been negligent and unsuccessful at protecting owners/operators sensitive information. One glaring example occurred when the DHS Cybersecurity & Infrastructure Security Agency's (CISA) Chemical Security Assessment Tool (CSAT)[19] was successfully hacked and compromised for multiple days before CISA realized the breach had occurred. The CSAT contains chemical facility security vulnerabilities and plans that owners/operators were mandated to submit.

Given the significant implications of the CSAT breach, it is imperative to address the need for all Government entities, including TSA, to be held accountable for the collection, aggregation, and protection of sensitive operations information. What were at one time considered adequate cybersecurity measures for the CSAT data storage still resulted in a breach. Despite Government's stringent safeguards and robust incident response protocols, no systems are impenetrable. Effective oversight and enhanced security frameworks on the Government's own networks are essential to protect national security interests and not create risks for the owners/operators. More importantly, Government should ask itself, "why is possession of sensitive private-sector operational information necessary?" AGA and its member companies value Government partnership but also seek to limit the vulnerabilities introduced by demonstrably subpar Government cybersecurity performance.

Cybersecurity Reciprocity and Harmonization

Cybersecurity harmonization has become a catchphrase that deserves to be placed in perspective. While applicable for cybersecurity assessments and cybersecurity incident reporting, harmonization of cybersecurity regulations is a chokehold for any risk-based, outcome-focused cybersecurity regulatory approach. The majority (if not all) of existing cybersecurity regulations involve prescriptive, check-the-box compliance, which is simpler for the Government to measure than performance-based security. Given this landscape, harmonization approaches that do not explicitly endorse performance-based cybersecurity will fail to recognize the operational differences across the oil and natural gas value chains that drive the necessity of risk-based cybersecurity regulations. Along similar lines, Government-wide reciprocity for relevant agency-led cybersecurity inspections and audits would benefit sector regulators by reducing duplicative evaluations and help improve regulated communities' cyber readiness. Arguably, inspection reciprocity has greater potential than harmonization and can be acted on with less bureaucracy for all stakeholders.

IN CLOSING

America's natural gas utilities recognize their attractiveness as a vector and target for nefarious nation-state hackers and cyber criminals. AGA member utilities combat the threat daily by leveraging top-notch cybersecurity technologies and personnel and maintaining a productive security partnership with the Federal Government, in particular TSA. No single standard or prescriptive regulation can secure all pipeline systems along both the natural gas and oil value chains. TSA recognizes this and is admirably taking the more difficult—while more sound and effective—path of implementing performance-based cyber requirements that will be attainable

[18] No entity is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access. See Zero Trust Architecture, GSA, available at *https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/zero-trust-architecture#:?:text=Zero%20trust%20is%20an%20-approach,and%20enterprise%20infrastructure%20and%20workflows* (last visited November 15, 2024).

[19] Top-Screen Surveys, Security Vulnerability Assessments, Site Security Plans/Alternative Security Programs, Personnel Surety Program Data, and CSAT User Information.

and sustainable by the owners/operators and auditable by the regulator. AGA encourages the Government to learn from the successes of TSA in their genuine collaboration with industry owners/operators and encourages TSA to recount the security successes that result from proactive collaboration. Over the decades, TSA and pipeline owners/operators have carried a similar banner into battle in support of our common mission.

Mr. GIMENEZ. Thank you, Ms. Denbow.

Members will be recognized by order of seniority for their 5 minutes of questioning. I now recognize myself for 5 minutes.

Ms. Denbow, can you elaborate on your last statement? You seem to be, you know, heaping praise on TSA and the new regulations, hoping that new directives will be fewer and fewer. But then you ended up on kind-of a sour note, so I'd like to home in on that.

Can you elaborate on what you just said at the end?

Ms. DENBOW. Yes, sir, and thank you very much for your firefighting service. Appreciate that.

This has been an on-going point of contention between the pipeline sector and TSA, and I will tell you, we have a very positive relationship with TSA from over many, many—2 decades of working with them.

Our concern is that there seems to be this, like I said, fixation on the part of every Government entity, including TSA, that in order for them to prove that operators are doing what they're doing, or in order for the nonperformance-based regulations to check the box for compliance, the Government has to take control or possession of our sensitive operations-related information.

When I refer to that, I'm talking about specifically, example in the proposed rule, TSA talks about us submitting identification of critical cyber systems, specific network architecture, baseline communications, detailed measures to protect our critical cyber systems, measures to address response to, recovery from, and—from a cyber incident.

If we're going to give all of this to TSA for them to hold on to, we might as well just give it to China or to Russia because there is no storage system that—for data—that is impenetrable and from third-party—unauthorized third-party access to insider threat, which is my bigger concern. There is no reason for the Government to have to have possession of this information.

We have worked diligently with TSA, and as pointed out by the recent panelists, that they are coming on-site for on-site inspections. Yes, it takes longer for the inspections, but then it allows us to prevent that vulnerability of TSA taking possession of our critical information.

Mr. GIMENEZ. Do you have any—has TSA given you a reason why they require that? Because I actually agree with you that once you give it away to the Government, to us, there is no guarantee that an adversary nation-state can't access it through us, and therefore, put you at risk.

Why does TSA need this?

Ms. DENBOW. I don't necessarily think it's just TSA. I think it is a Federal Government and State government belief that in order for them to protect us, they need to have our critical information. It's our job as the owner-operator to protect us. It's TSA's and the Federal Government's job to protect the community, the Nation. We should be able to do that together without putting the owner-operators in a vulnerable position that they would otherwise not be if they do not have to share that information.

TSA's concern, as I understand it, has been the increased amount of time that they would have to spend on-site for inspections. While I recognize that and I do say that TSA does not have the resources that it needs, it is working diligently to really achieve all that it needs to.

But making an inspection on-site lasts for a couple of days longer so that my owner-operators can sleep better at night, not worried that an insider threat or a nation-state could hack into a system that has been proven through DHS, through DOE—name the 3-letter Government organization that has not been compromised. That is why.

Mr. GIMENEZ. Ms. Denbow, I think all entities can be compromised.

Ms. DENBOW. Yes.

Mr. GIMENEZ. At the end, no matter what we do, if somebody puts their mind to it, they can probably get into wherever it is that they want to get into.

Ms. DENBOW. Yes, Mr. Chairman.

I would like to add—I would like to add because it would be remiss if I didn't—TSA has gone above and beyond to try to protect this information, but we just have to accept the reality that nothing is impenetrable.

Mr. GIMENEZ. Because of that I've always—my belief is that, yes, we try to put up as many safeguards as possible so that there's no penetration and no corruption. However, I'm more inclined to say, OK, assume that you are corrupted and assume that you are attacked, how can you get back to operations as quickly as possible knowing that you will be attacked, and that you will be disabled?

So our—my problem with the entire cyber world is our overreliance on it, and also, the lack of institutional knowledge of how to operate things without technology, the old-fashioned way, because we may have to resort to that. Unfortunately, we just keep becoming more and more reliant on electronic systems, on digital systems where we're becoming more and more vulnerable to it. That's my problem.

Anyway, my 5 minutes are up.

I now recognize the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Jeffries, regulations that are meant to enhance security should not be all really burdensome, and we're going to get to the gentlelady's point, because I think that's an important conversation. But regarding rail, the operation of our rail systems is absolutely critical to the performance of our Nation. The historical significance of rail systems working in a cooperative manner with every sovereign State's government and local municipalities, and with operating under Federal regulation and with thousands and thousands of industry stakeholders that are required to plug into the rail systems, it's quite a complex thing when you really look at it.

So the regulations that the Federal Government places upon you, intended to enhance security, yes, of course, but my assessment is that it's far too burdensome and can interfere with business as, again, as the gentlelady pointed out.

But how does that relate to financial costs? Do you find that in your interactions with TSA and the effort to enhance security regulations and cyber threat for rail, is there fair and due consideration given to the financial impact in the rail industry?

Mr. JEFFRIES. Well, thank you, Congressman, for the question.

You know, we've been at this a long time. You kind-of referenced that, about 200 years of——

Mr. HIGGINS. Right.

Mr. JEFFRIES [continuing]. Moving things around the country and doing it to a high degree of safety. We take our responsibility with the utmost of seriousness to move goods safely and securely, because we move all variety of goods that Americans rely on every single day. Cybersecurity is a key portion of that, and as I mentioned, we've been at that since before the year 2000, in advance of Y2K, and we have had a productive relationship overall with the TSA. Certainly can't say that for every Government agency, so it's worth highlighting that.

But, to your point, we've got to be—we've got to think about the cost-benefit equation. So, to my colleague's point, are we spending more time checking boxes and fulfilling requirements for requirements' sake, or are we maximizing security for maximizing security's sake? Certainly there's a cost of—there's a financial cost. There's a human resource cost. There's a physical and digital asset cost——

Mr. HIGGINS. So is that fairly evaluated is my question? In your interaction with TSA, is the financial impact fairly evaluated?

Mr. JEFFRIES. So I would say it's acknowledged. Whether or not it's fairly evaluated, I'll let you know when we file our comments once we get through this massive rule.

Mr. HIGGINS. OK. Well, I'll take that as your answer. Be reassured, and for your partners across the country, and we are watching that. I mean, the financial impact is significant, and it has to be part of the formula.

Mr. JEFFRIES. I would quickly say that I think that's why it's so important that you have a designated problem you're trying to solve, an outcomes-based approach versus an inputs-based approach. So, that's a core philosophy of ours and——

Mr. HIGGINS. Well, that's a common-sense answer, so I'm not sure that's allowed in the District of Columbia.

Mr. JEFFRIES. OK. Fair enough.

Mr. HIGGINS. Ms. Denbow, quoting you, you said that the Government essentially seeks control or possession of your critical infrastructure systems, and you're saying that in order for the Government to check your cybersecurity compliance, the Government is compromising your cybersecurity infrastructure. This is exactly the conservative perspective of Government overreach. So would you please expound upon that? What would be your suggestion to the Federal Government to get the hell out of your way unless you protect your systems?

Ms. DENBOW. Thank you for that colorful opening.

AGA, the American Gas Association, we support reasonable cybersecurity regulations. From the natural gas utility perspective, we do not just have to answer to the Federal Government. We also answer to their State Public Utility Commission, and for that, we have—we are required to do long-term planning. So we need a system. We need reasonable regulations that are not constantly changing so that we can do that long-term planning and justify the expenses for the sake of security.

We applaud TSA for sticking with the performance-based approach. What we need TSA to do is to rely on the fact that, No. 1, reasonable cybersecurity regulations have to be attainable. The operators have to be able to achieve them. They have to be sustainable. The operators have to be able to sustain them and keep them going. Otherwise, it's wasted money. Then TSA feels that last part is for them to be auditable. That's the part where we're always rubbing—where we're always bumping heads, and that is because there are ways where TSA can audit and verify without having to take possession of our critical infrastructure information.

Mr. HIGGINS. Because when you say taking possession, you mean to document your security mechanisms you have in place, and therefore, they're exposing your security mechanisms themselves to breach by the cyber threat operators and bad actors across the world. Is that essentially what you're saying?

Ms. DENBOW. In a nutshell, basically it is, rather than showing what they would like is to get a copy. As soon as—we have no problems showing TSA that information. Where the challenge is is when that information physically or electronically leaves our environment.

Mr. HIGGINS. I understand. You have my commitment to address that. That's precisely the kind of thing we intend to push back against.

Mr. Chairman, my time has well expired. Thank you for this hearing. I yield.

Mr. GIMENEZ. Thank you to the gentleman from Louisiana.

I want to thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may have some additional questions for the witnesses, and we would ask the witnesses to respond to these in writing. Pursuant to committee rule VII(D), the hearing record will be open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:17 a.m., the subcommittee was adjourned.]

APPENDIX

Statement of Airlines For America

November 19, 2024

On behalf of our members,[1] Airlines for America (A4A) submits this written testimony for the record for the House Homeland Security Committee's hearing on Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector. We thank the committee for holding this important hearing because harmonizing cybersecurity requirements and improving information sharing across the Federal Government is much-needed and long-overdue.

A4A supports policies and measures that promote safety, security, and a healthy U.S. airline industry, including those dealing with cybersecurity. Cybersecurity is increasingly important to aviation safety and security. It requires effective policies, practices, and processes, as well as shared, mutual cybersecurity goals among air carriers, Congress, and the rest of the Federal Government. As an industry with multiple Federal regulators, we are concerned with the lack of harmonization of cybersecurity requirements across Federal agencies especially when agencies use their emergency authorities bypassing traditional interagency coordination. We believe that improving harmonization of Federal policies will lead to better outcomes for both the private and public sectors.

A4A believes that protecting critical infrastructure requires consistent, streamlined, and harmonized cybersecurity requirements. Therefore, we strongly encourage Congress and the administration to prioritize the harmonization of both cybersecurity incident reporting and mandatory cybersecurity measures, especially before introducing any new requirements. The current practice of requiring multiple reports with different reporting triggers and standards to different Federal agencies is a significant and unnecessary burden on industry that materially reduces the effectiveness of voluntary and mandatory reporting frameworks to combat cybersecurity risks.

A4A also supports efforts to improve information sharing among Federal agencies and between the private and public sectors. There is no "silver bullet" for addressing cybersecurity risks, but rather, the best, mature cybersecurity programs are risk-based, threat-informed, and constantly evolving to stay ahead of a dynamic threat landscape. This must include a strong partnership of information sharing with the Federal Government and other stakeholders to ensure critical infrastructure sectors stay ahead of evolving cybersecurity threats.

TRANSPORTATION SECURITY ADMINISTRATION (TSA) CYBERSECURITY REQUIREMENTS

Over the past 3 years, TSA has issued a number of cybersecurity provisions under its standard security program for aviation operators. These include Change 66 and Change 27 to the Standard Security Program,[2] [3] Joint Emergency Amendment (Joint EA),[4] Policy Clarification Notice (Critical Systems),[5] and Joint National Alter-

[1] See A4A's members are: Alaska Air Group, Inc.; American Airlines Group, Inc.; Atlas Air Worldwide Holdings, Inc.; Delta Air Lines, Inc.; FedEx Corp.; JetBlue Airways Corp.; Southwest Airlines Co.; United Airlines Holdings, Inc.; and United Parcel Service Co. Air Canada is an associate member.

[2] Change 66 to Aircraft Operator Standard Security Program, June 30, 2022.

[3] Change 27 to Full All Cargo Aircraft Operator Standard Security Program, June 30, 2022.

[4] Joint Emergency Amendment 23–01, *Cybersecurity—Performance-Based Measures,* March 07, 2023.

[5] Transportation Security Administration Policy Clarification Notice, Critical Systems, September 8, 2023.

native Measure (Joint NAM) 23–01.[6] The requirements within these documents form the foundation of TSA's aviation cybersecurity regulatory framework.

Although TSA's use of emergency authorities to issue the Joint EA and Joint NAM did not provide airlines the opportunity to comment, TSA has conducted industry outreach, including Classified briefings. Reflecting industry's input, TSA modified its traditional physical security processes to account for the significant differences between cybersecurity and physical security. Over the past 6 months, TSA has also taken the lead in establishing an interagency information sharing working group focused on the unique information and intelligence needs of the aviation sector. TSA is also co-leading a new Cybersecurity Policy Working Group with A4A, providing a forum for our members to better understand TSA's compliance requirements, as well as develop recommendations for future changes to TSA's regulatory program.

This is an example for other Federal agencies on how meaningful collaboration can ensure critical sectors stay ahead of the evolving cybersecurity threat environment. We believe the best regulatory frameworks are those that incorporate stakeholder collaboration, use accepted industry standards, are agile, risk-based, and threat-informed. However, the Federal Government's overall cybersecurity regulatory approach lacks harmonization and needs better information sharing to ensure all critical infrastructure sectors stay ahead of threat actors.

FEDERAL CYBERSECURITY DIS-HARMONY—INCIDENT REPORTING

In the Department of Homeland Security's (DHS) report, Harmonization of Cyber Incident Reporting to the Federal Government,[7] the authors identified 45 Federal cybersecurity incident reporting requirements currently in effect. They also identified 7 proposed rules, 5 potential new requirements under consideration, and 1 future rule (Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)). It serves as a stark reminder of the Federal bureaucracy's "seemingly insatiable appetite for data" that Congress has quelled in the past.[8] In fact, other than CIRCIA, none of the 58 final or proposed cybersecurity incident reporting requirements address harmonization or contemplates streamlining reporting requirements across Federal agencies.

Although the aviation industry is not subject to all 58 reporting requirements, airlines are currently subject to 10 different Federal departments and agencies existing or proposed, mandatory and voluntary incident-reporting frameworks. These Federal agency and department frameworks include:

1. *Federal Aviation Administration (FAA).*—Mandatory Reporting (Advisory Circular 119–1A, "Aircraft Network Security Program," 28 September 2023);
2. *Transportation Security Administration (TSA).*—Mandatory Reporting (Standard Security Program Change, 10 January 2022);
3. *Department of Defense (DoD).*—Mandatory Reporting (Defense Federal Acquisition Regulations Supplement (DFARs) 252.204–7012 and 10 U.S.C. § 391—U.S. Code—Unannotated Title 10. Armed Forces § 391);
4. *U.S. Transportation Command (USTRANSCOM).*—(General Cyber Security Requirements in USTRANSCOM contracts, Civil Reserve Air Fleet, Appendix 6);
5. *Customs and Border Protection (CBP).*—Mandatory Reporting (Cargo Systems Messaging Service (CSMS) No. 5285040—"Reporting a Cybersecurity Event to CBP," 12 September 2022 and CSMS No. 60261003);
6. *Security and Exchange Commission (SEC).*—Mandatory Reporting *(Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (In Effect on September 5, 2023)):
7. *Cybersecurity and Infrastructure Security Agency (CISA).*—Voluntary Reporting *(Cybersecurity Information Sharing Act (CISA) of 2015),* pending mandatory reporting *(Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) of 2022);
8. *General Services Administration (GSA).*—Mandatory Reporting ((Federal Acquisition Regulations (FAR) subpart 4.4 & 52.204–232, C.F.R part 117) & (32 C.F.R 117.8));
9. *Federal Bureau of Investigation (FBI).*—Voluntary Reporting (Report a Crime or Fraud);

[6] Joint National Alternative Measure 23–01A, *Alternative Measures for Certain Requirements in Joint EA,* February 28, 2024.

[7] DHS Congressional Report, *Harmonization of Cyber Incident Reporting to the Federal Government,* September 19, 2023.

[8] See *Dole* v. *United Steelworkers,* 494 U.S. 26, 32 (1990).

10. National Aeronautics and Space Administration (NASA).—Mandatory Reporting ((FAR subpart 4.4 & 52.204–232, C.F.R part 117) & (32 C.F.R 117.8)); and

it is important to note, these 10 different Federal requirements differ on definitions, thresholds, processes, time lines, data protections, compliance regimes, and content requirements. We doubt that the Federal Government intended to create an environment where 58 cybersecurity incident reporting frameworks with divergent requirements are in effect, but this is the environment that regulated entities must currently navigate to ensure compliance. For sectors like transportation with numerous regulators and relationships across sectors, this complex patchwork of unharmonized cybersecurity incident reporting requirements is especially burdensome.

Finally, harmonization of cybersecurity incident reporting is a good first step, but harmonization of mandatory cybersecurity measures and compliance frameworks is also critically important. A4A supports the Office of the National Cyber Director's (ONCD) efforts to harmonize cybersecurity requirements across the Federal Government. Representative Higgins' recent proposal, H.R. 10123, the Streamlining Federal Cybersecurity Regulations Act, is also promising, as it is intended to address the challenges associated with multiple regulatory regimes by establishing an interagency Harmonization Committee at the ONCD. Ensuring all mandatory requirements are risk- and threat-based, streamlined, and harmonized is in the best interest of regulators and operators, and it will lead to the best outcomes and drive down risk. If harmonization is not possible, then agencies should support a reciprocity framework that reduces unnecessary burdens and allows regulated parties to prioritize critical resources on a threat-based, risk-informed approach.

Information Sharing.—The industry supports and engages in a strong partnership of information sharing with the Federal Government and other stakeholders. Specifically, A4A members participate in and contribute to regular and frequent engagements with:

- ONCD, FAA, DHS, TSA, CISA, DoD, law enforcement, the intelligence community, and other agencies;
- The Defense Industrial Base, National Defense Transportation Association, Aviation Information Sharing and Analysis Center (A–ISAC), International Air Transport Association (IATA), International Civil Aviation Organization (ICAO), and other cyber-related communities; and
- With the Original Equipment Manufacturers (OEMs) to further understand and address possible threats.

As noted, our industry also appreciates TSA leading the establishment of an interagency information-sharing working group focused on the aviation sector. We look forward to participating and providing recommendations to strengthen and improve information-sharing processes. We believe that information sharing among aviation regulators, the intelligence community, and private stakeholders is foundational to the safety, security, and resiliency of the transportation system aviation subsector. Information sharing is necessary for both:

- Near-real-time intelligence and information used to protect aviation systems from existing and emerging threats; and
- To inform policy development, verify the effectiveness of policy outcomes, and determine if policy changes are necessary to stay ahead of evolving threats and risks.

Although Federal agencies have made strides to improve information sharing such as multi-agency threat bulletins, information sharing among Federal agencies and with the aviation sector needs to improve. The information airlines receive from Federal agencies is often not timely or consistent. Additionally, it is not clear that processes exist to rapidly update regulatory requirements at a speed necessary to stay ahead of evolving threats. We look forward to continuing to work with aviation regulators, the intelligence community, and Congress to improve information sharing.

HARMONIZATION AND INFORMATION-SHARING RECOMMENDATIONS

While we are encouraged by recent ONCD and CISA efforts to discuss harmonization across the Federal Government, we believe much more can and should be done. Specifically, we recommend the following actions:

- Create and adopt a single reporting framework that includes agreed-upon reporting definitions, threshold, process, time line, data protection, compliance regime, and content requirements. Although we have concerns with the current CIRCIA proposal, it could serve as the Federal Government's single reporting framework.

- The administration, independent regulators, and Congress should prioritize cybersecurity incident reporting harmonization before any new cybersecurity requirements are implemented including proposed regulations or legislation for contractors who handle Federal information.
- Congress should remove any legal or statutory barriers to harmonization.
- The administration and Congress should work with industry to pass legislation that balances regulatory compliance with consensus standards and incentives.
- Congress should pass legislation authorizing a Presidential designee to convene independent regulatory agencies to exchange best practices and coordinate cybersecurity incident reporting.
- Provide CISA with the necessary resources to implement CIRCIA and any future statutory incident reporting requirements.
- Increase funding to Federal agencies to increase the number of industry members for a Top-Secret clearance. Sharing timely, relevant information requires all parties to have access to the right information.

CONCLUSION

Critical infrastructure sectors are best positioned when cybersecurity regulations and oversight are consistent across the Federal Government. The best cybersecurity programs are those that are threat- and risk-based, data-informed, outcome-focused, and flexible enough to address evolving threats. The current state of cybersecurity incident reporting and broader cybersecurity regulatory dis-harmonization was created by the Federal Government, but the Federal Government is also uniquely positioned to harmonize its requirements, however, it will take a concerted effort by many to efficiently and effectively put in place a harmonized framework. Information sharing can improve as well, but it will require a renewed focus and prioritization by Federal agencies.

Thank you for the opportunity to raise concerns and provide recommendations to improve Federal harmonization of cybersecurity incident reporting. We stand ready to work with the committee and other stakeholders to find practical solutions to enhance cybersecurity.