United States Government Accountability Office

Testimony

Before the Subcommittee on Transportation and Maritime Security, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, November 19, 2024

SURFACE TRANSPORTATION

TSA Is Taking Steps to Enhance Cybersecurity, but Additional Actions Are Needed

Statement of Tina Won Sherman, Director,
Homeland Security and Justice

GAO-25-107947

GAO Highlights

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

November 19, 2024

SURFACE TRANSPORTATION

TSA Is Taking Steps to Enhance Cybersecurity, but Additional Actions Are Needed

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 six 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 one recommendation, partially addressed one recommendation, and has not implemented four recommendations. GAO will continue to monitor the agency's progress.

View GAO-25-107947. For more information, contact Tina Won Sherman at (202) 512-8461 or shermant@gao.gov, or David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov.

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 five 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

[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.

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 cyberattacks 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 cyberattacks 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 cyberattacks in the event of a major crisis or conflict with the U.S.[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

[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 three U.S. military bases. Microsoft, which first detected the hacking, noted that the operation's likely aim was to disrupt critical communications between the U.S. and Asia region during a future crisis.

degree of confidence that the attackers would be able to move from IT networks to operational technology assets and disrupt critical functions.

Federal Cybersecurity Challenges

In June 2024, we reiterated the importance of addressing four 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 four critical infrastructure sectors that reported almost half of all ransomware attacks—critical manufacturing, energy, healthcare 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

[5]GAO, *High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation*, GAO-24-107231 (Washington, D.C.: June 13, 2024). We reported that the federal government needed to address four 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 four 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, D.C.: 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.

activities, which, according to the Memorandum, should include recommending sector-specific measures to protect critical infrastructure.[8]

TSA is one of DHS's two 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 five 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 stakeholder input and feedback. An interagency oversight body has also reviewed and approved these directives after issuance.[12] Of the five directives, three directives have requirements, such as cybersecurity incident reporting, to enhance

[8]White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum-22 (Washington, D.C.: 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(*l*)(2)(A).

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

[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.

cybersecurity in each transportation mode. The remaining two directives impose additional requirements for cybersecurity mitigation actions and testing across the modes.

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.

[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, D.C.: 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.

TSA's proposed rule is a recent example of a federal effort to put forth requirements to mitigate and report cyberattacks. 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 four 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 six 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 one recommendation, partially addressed one recommendation, and has not implemented four 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.

[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, D.C.: July 30, 2024).

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

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

Table 2: GAO Recommendations to the Department of Homeland Security or Transportation Security Administration for Improvements to Transportation Systems Sector Cybersecurity, as of November 2024

GAO Report Area and Year	Recommendation summary	Status
Ransomware risk reduction 2024[a]	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[b]	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[c]	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[d]	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

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

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

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

[d]GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, D.C.: 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

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

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

[21]GAO, *Priority Open Recommendations: Department of Homeland Security*, GAO-20-355PR (Washington, D.C.: 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, D.C.: June 5, 2019).

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 cyberattack, 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 pipeline owners and operators that require certain actions to improve cybersecurity preparedness. The actions include appointment of cybersecurity coordinators, reporting of cybersecurity

[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, D.C.: Dec. 1, 2022).

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

[26]Department of Homeland Security, Transportation Security Administration, *Enhancing Rail Cybersecurity*, Security Directive 1580-21-01 (Springfield, V.A.: 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, V.A.: 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, Virginia: 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, V.A.: 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.

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.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Tina Won Sherman, Director, Homeland Security and Justice, at (202) 512-8461 or shermant@gao.gov, or David B. Hinchman, Director, Information Technology and Cybersecurity, at (214) 777-5719 or hinchmand@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this statement are Ben Atwater (Assistant Director), Joshua Leiling (Assistant Director), and Luis E. Rodriguez (Analyst-in-Charge). Other staff who made key contributions to the reports cited in the testimony are identified in the source products.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, X, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548