Congressional Research Service
Informing the legislative debate since 1914

Transportation Security: Background and Issues for the 119th Congress

May 23, 2025

Congressional Research Service
https://crsreports.congress.gov
R48543

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Transportation Security: Background and Issues for the 119th Congress

The nation's aviation, mass transit, passenger and freight rail, maritime, and pipeline transportation systems are geographically dispersed and designed for accessibility and efficiency. These characteristics make them vulnerable to attack. While securing the transportation sector is difficult, measures can be taken to deter attackers. A key challenge facing Congress is how to implement and finance a system of deterrence, protection, and response that effectively reduces the likelihood and mitigates the consequences of attacks without interfering with travel, commerce, and civil liberties.

Transportation security has been a major policy focus since the terrorist attacks of September 11, 2001. In the aftermath of those attacks, Congress passed the Aviation and Transportation Security Act (ATSA; P.L. 107-71). ATSA established the Transportation Security Administration (TSA), mandated federal screening of airline passengers and their baggage, and ordered the deployment of air marshals on all high-risk commercial passenger flights. Congress has since passed legislation intended to further enhance transportation security measures. The FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) and the TSA Modernization Act (P.L. 115-254, Division K) included provisions intended to improve screening technologies, streamline passenger screening, mandate more rigorous background checks of airport workers, strengthen airport access controls, increase passenger checkpoint efficiency, and enhance security in public areas of airports and at foreign airports where flights depart for the United States.

Numerous challenges remain regarding aviation and transportation security, including

- developing and deploying capabilities, including the potential use of biometrics, to verify the identities of transportation workers and travelers;
- developing risk-based approaches to vetting and screening transportation workers who access secured areas of airports and other sensitive areas of transportation networks;
- developing cost-effective solutions to screen air cargo and freight without impeding the flow of commerce; and
- improving coordination among state, local, and federal homeland security and law enforcement personnel to deter and respond to criminal and terrorist acts targeting public areas of transportation facilities.

These options and oversight of TSA's potential actions to implement them may be of interest to the 119th Congress. Topics may include

- considering the federal role in airport screening;
- funding aviation security functions, such as passenger and baggage screening;
- assessing the evolution of screening technologies and emerging screening technology solutions;
- using terrorist watch lists to deny boarding to flagged individuals and identify individuals for enhanced security screening while respecting civil liberties;
- improving processes and programs, including known traveler programs, to streamline and expedite air traveler screening;
- addressing data security and privacy concerns surrounding the use of biometrics;
- implementing approaches, regulations, and international agreements to conduct risk-based screening of air cargo shipments worldwide;
- protecting public areas of airports;
- developing countermeasures to protect critical infrastructure, including airports and aircraft, from attacks and interference from drones and possible terrorist attacks using shoulder-fired missiles; and
- developing cybersecurity measures to protect infrastructure and operations across all transportation modes.

SUMMARY

R48543

May 23, 2025

Bart Elias, Coordinator
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

Ben Goldman
Analyst in Transportation Policy

Chris Jaikaran
Specialist in Cybersecurity Policy

Jennifer J. Marshall
Analyst in Transportation Policy

Paul W. Parfomak
Specialist in Energy Policy

Contents

Tables

Contacts

Introduction

The nation's aviation, mass transit, passenger and freight rail, maritime, and pipeline transportation systems are geographically dispersed and designed for accessibility and efficiency. While these characteristics make them vulnerable to attack, measures can be taken to enhance security and deter attackers. One focus of policy debate is how to implement and finance a system of deterrence, protection, and response that would reduce the likelihood and mitigate the consequences of terrorist attacks without unduly interfering with travel, commerce, and civil liberties.

For all modes of transportation, four principal policy objectives aim to support a system of deterrence and protection: (1) ensuring the trustworthiness of the passengers and the cargo flowing through the system; (2) ensuring the trustworthiness of transportation workers with unique access to transportation vehicles and infrastructure; (3) ensuring the trustworthiness of the private companies that operate in the system, such as the carriers, shippers, agents, and brokers; and (4) establishing physical and cybersecurity measures around transportation facilities and vehicles to address vulnerabilities and detect and mitigate threats.

The first three policy objectives are concerned with preventing attacks from within a transportation system, such as the terrorist attacks of September 11, 2001 (9/11 attacks). The main concern is that terrorists could gain access to the system and launch an attack by posing as legitimate passengers, shippers, or authorized workers.

The fourth policy objective is concerned with preventing an attack launched from outside a transportation system. For instance, terrorists could ram a bomb-laden speedboat into an oil tanker, as was done in October 2002 to the French oil tanker *Limberg*, or they could shoot a shoulder-fired missile at an airplane during takeoff or landing, as was attempted in November 2002 against an Israeli charter jet in Mombasa, Kenya.

Achieving all four objectives would be challenging or practically impossible for some transportation modes. Policymakers may find it difficult to evaluate limited or suboptimal options to minimize the consequences of an attack without imposing requirements that could impede the flow of persons and goods through the nation's transportation networks. This report discusses the various physical security and cybersecurity measures and approaches implemented or under consideration to address these objectives across major modes of transportation, including aviation, transit and passenger rail, freight rail, ports and maritime transport, and pipelines.

Aviation Security[1]

Following the 9/11 attacks, Congress enacted the Aviation and Transportation Security Act (ATSA; P.L. 107-71), creating the Transportation Security Administration (TSA) and mandating that security screeners employed by the federal government inspect airline passengers and their baggage and deploy air marshals on all high-risk commercial passenger flights. The legislation placed TSA within the U.S. Department of Transportation (DOT). In 2003, TSA was transferred to the newly formed Department of Homeland Security (DHS).[2] Although TSA has primary responsibility for overseeing security across all transportation modes, its budget, personnel, and resources are dedicated to addressing aviation security, particularly the security of scheduled commercial passenger flights. Historically, aviation security activities have accounted for more

[1] This section was prepared by Bart Elias, CRS Specialist in Aviation Policy.

[2] See Homeland Security Act of 2002 (P.L. 107-296).

than 95% of TSA's total budget, and aviation screening operations make up roughly two-thirds of TSA appropriations.

Over the past two decades, aviation security legislation has largely focused on specific mandates to comprehensively screen for explosives and carry out background checks and threat assessments of passengers and air cargo shipments. Despite the continued focus on aviation security, numerous challenges remain, including

- addressing the federal role in airport screening and controlling associated costs;
- screening passengers, baggage, and cargo for explosives threats;
- developing risk-based methods for screening passengers and others with access to aircraft and sensitive areas of airports;
- verifying identities such as via approved identification or biometrics;
- utilizing available intelligence information and watch lists to identify individuals who may pose threats to civil aviation;
- implementing systems, regulations, and international agreements to assess risk and conduct risk-based screening of air cargo shipments worldwide;
- deterring and responding to security threats in public areas of airports and at screening checkpoints;
- addressing aircraft vulnerabilities to shoulder-fired missiles and other external threats, such as rocket-propelled grenades; and
- addressing the potential security implications of unmanned aircraft operations in domestic airspace and developing countermeasures to protect critical infrastructure, including airports and aircraft, from drone intrusions or attacks.

Federalized Airport Screening

The extensive federal role in airport screening has been part of the commercial air passenger experience in the United States for more than two decades, reflecting TSA's statutory responsibilities for these functions. In some other countries, air passenger and baggage screening are airport or airline responsibilities frequently carried out by contract personnel.[3] In other countries, such as Canada, government-backed corporations are responsible for passenger, baggage, and cargo screening.[4]

In general, all commercial airline passengers and baggage must be physically screened prior to boarding a flight.[5] For flights originating in the United States, the screening generally must be carried out by federal screeners. As an exception, personnel employed by a qualified private screening company operating under the statutory framework of the TSA Screening Partnership Program (SPP) may also perform screening at designated SPP airports.[6] While any commercial airport in the United States may opt out of federal screening, private screening under the SPP currently includes 21 airports out of approximately 440 commercial passenger airports where

[3] Shirley Ybarra and Robert W. Poole, *Overhauling U.S. Airport Security Screening*, Reason Foundation, Policy Brief 109, July 2013, https://reason.org/wp-content/uploads/files/overhauling_airport_security.pdf.

[4] Canadian Air Transport Security Authority, https://www.catsa-acsta.gc.ca/en/publications/canadian-air-transport-security-authority.

[5] 49 U.S.C. §44901.

[6] 49 U.S.C. §44920.

passenger and baggage screening operations are required.[7] The TSA Modernization Act, incorporated into the FAA Reauthorization Act of 2018 (P.L. 115-254, Division K), includes language directing TSA to streamline the contracting process for private screening at airports and directs TSA to look into the feasibility of modifying the SPP to allow individual airport terminals, instead of entire airports, to switch over to screening by private contractors.[8]

Some Members have proposed legislation seeking more extensive reforms of passenger screening, but those bills have not been extensively debated in Congress. In 2006, a proposal (H.R. 4439, 109th Congress) sought to establish a performance-based federal organization, to be called the Airport Screening Organization, that would have taken over responsibility for managing the day-to-day passenger and baggage screening functions performed by TSA. The bill proposed that the screening organization would be managed similarly to a business, with a chief operating officer at the helm who would be responsible for developing and overseeing a strategic plan with measurable performance goals to track effectiveness, efficiency, and productivity. The bill sought to provide additional incentives to airports requesting to join the SPP and to private screening companies approved to provide screening services to SPP airports that meet or exceed performance expectations. More recently, the Screening Partnership Reform Act (S. 890, 118th Congress) proposed modifications to the SPP that would have given airports more direct control over selecting qualified private screening companies and streamlined transitions from TSA screening to SPP contract screening operations.

Recent policy reports have reinvigorated discussion of broader initiatives to reform security screening operations at airports. The Project 2025 Presidential Transition Project's *Mandate for Leadership* report asserts that TSA, or at least its airport screening functions, should be "privatized."[9] It argues that this could be accomplished by expanding the SPP to all airports. Alternatively, the report offers that TSA could adopt a system similar to Canada's, in which a government-backed corporation performs screening operations. Under such scenarios, TSA could continue to exist to set regulations and conduct oversight to evaluate regulatory compliance. The report asserts that such reforms could result in a 15%-20% savings compared with the existing aviation screening budget. A 2015 report published in the *Journal of Air Transport Management* analyzed annual aviation security costs, finding that between 2005 and 2014, the United States spent $9.92 per capita more than Canada on aviation security.[10] On a per passenger basis, the data indicated that total aviation security costs in the United States were roughly 16%-17% higher than in Canada. Achieving comparable reductions to aviation security costs in the United States may require modifications to the existing SPP statute, which mandates that compensation and other benefits for private screeners working under the SPP be equal to or greater than that of TSA screeners.[11] While labor costs are major contributors to aviation security spending, a 2013 policy analysis published by the Cato Institute concluded that TSA's workforce management problems and its history of deploying costly and unproven new technologies also have contributed to increased TSA spending.[12] Although it is unclear whether this is still an accurate portrayal of

[7] Transportation Security Administration (TSA), "Screening Partnership Program," https://www.tsa.gov/for-industry/screening-partnerships.

[8] P.L. 115-254, §1946.

[9] Paul Dans and Steven Groves, eds., *Mandate for Leadership: The Conservative Promise*, Project 2025 Presidential Transition Project (The Heritage Foundation, 2023).

[10] David Gillen and William G. Morrison, "Aviation Security: Costing, Pricing, Finance, and Performance," *Journal of Air Transport Management*, vol. 48 (September 2015), pp. 1-12.

[11] 49 U.S.C. §44920(c).

[12] Chris Edwards, *Privatizing the Transportation Security Administration*, Cato Institute, Policy Analysis no. 742, November 19, 2013.

TSA, potential nonlabor cost reductions may yield potential savings from proposed aviation security reforms.

TSA's budget for airport security screening has risen in response to targeted pay increases for TSA screeners that went into effect in July 2023. According to TSA, this action was taken to reduce screener attrition and improve morale; annual attrition at the agency has since dropped from nearly 20% to roughly 11%, and employee satisfaction has improved.[13] TSA hired 11,000 screeners in 2018 in response to the combination of attrition and increased passenger volume, but its hiring needs dropped to 9,000 in 2023. TSA argues that the drop in attrition has allowed for more selective hiring. The 2023 pay raises increased TSA's budget for its screening workforce from roughly $4.16 billion in FY2022 to $4.71 billion in FY2023 and in FY2024. The pay raises were championed by organized labor representing TSA screeners. The FY2025 budget proposed by the Biden Administration sought an additional increase, proposing to raise screener workforce funding to roughly $6.49 billion to cover a proposed 5.1% increase in the number of federal screeners to support a projected 9.2% increase in passenger volume.[14] The Full-Year Continuing Appropriations and Extensions Act, 2025 (P.L. 119-4), specified an overall increase to TSA's Operations and Support account, under which the screening workforce funding falls, of roughly $1.50 billion—about 16% more than FY2024 annualized amounts, but less than the requested increase of $2.4 billion proposed by the Biden Administration. The act does not specify what amount of this funding would be allocated for the screener workforce. However, the FY2026 discretionary budget request specifies a proposed reduction of $247 million compared with the FY2025 enacted amount for TSA screening.[15]

Historically, collective bargaining rights for TSA screeners has been a contentious issue. Most federal workers are covered under statutory provisions granting collective bargaining rights, but ATSA gave the TSA administrator broad discretion over whether or not to grant those rights for airport screeners. A 2003 determination by then-TSA Administrator James Loy concluded that collective bargaining rights for screeners were contrary to TSA's need for flexibility to counter evolving terrorist threats, such as the ability to quickly make changes to work schedules and other conditions of employment. Despite legal challenges, both the U.S. Federal Labor Relations Authority and courts have upheld TSA's 2003 determination, finding that TSA screeners have no statutory right to collective bargaining.[16] In 2011, reflecting changing Administration views about collective bargaining and labor representation, TSA screeners were afforded limited collective bargaining rights and job protections, which have been detailed in formal memoranda issued by various TSA administrators.[17] DHS ended collective bargaining rights for TSA screeners on March 7, 2025, asserting that collective bargaining constrained TSA's mission to safeguard transportation systems and that eliminating it would strengthen workforce agility, productivity,

[13] Testimony of TSA Administrator David P. Pekoske in U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, *An Examination of the Transportation Security Administration's Fiscal Year 2025 Budget*, 118th Cong., 2nd sess., H.Hrg. 118-64, May 15, 2024.

[14] Department of Homeland Security (DHS), *Transportation Security Administration Budget Overview, Fiscal Year 2025 Congressional Justification*, April 2024, https://www.dhs.gov/sites/default/files/2024-04/2024_0318_transportation_security_administration.pdf.

[15] Office of Management and Budget, *Fiscal Year 2026 Discretionary Budget Request*, May 2, 2025, https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf.

[16] See U.S. Dep't of Homeland Security Border and Transportation Security Directorate Transportation Security Admin. and Am. Fed'n of Gov't Employees AFL-CIO, 59 F.L.R.A. 423 (2003); Am. Fed'n of Gov't Employees, AFL-CIO v. Loy, 281 F. Supp. 2d 59 (D.D.C. 2003).

[17] For example, see Letter from TSA Administrator John S. Pistole to all TSA employees, February 4, 2011; and TSA Administrator David P. Pekoske, *Determination on Transportation Security Officers and Collective Bargaining*, July 3, 2019.

resiliency, and innovation.[18] It has been reported that the decision to end collective bargaining rights will not impact recent TSA pay raises.[19]

Funding Aviation Security and TSA Screening Functions

Congress has considered how to control and allocate costs for aviation security, particularly TSA passenger and baggage screening functions. ATSA authorized a security service fee, often referred to as the "9/11 security fee" or passenger security fee, that is collected from commercial airline passengers to offset some of the costs associated with providing civil aviation security services.[20] Those fees have increased twice since inception, the last time being in 2014 when they were raised to $5.60 per passenger for each one-way trip, with a cap of $11.20 per round-trip flight. With that increase, included in the Bipartisan Budget Act of 2013 (P.L. 113-67), the statute stipulated that a specified dollar amount of the fees collected be deposited into the Treasury General Fund each fiscal year and applied toward debt reduction. The statute originally specified such amounts through FY2023, but the requirements for specified amounts to be deposited into the Treasury General Fund were extended though FY2025 by a provision in P.L. 114-41. The amount for FY2025 is $1.6 billion. This was further extended by a provision in the Bipartisan Budget Act of 2018 (P.L. 115-123) that specifies amounts of $1.64 billion for FY2026 and $1.68 billion for FY2027; no amounts are specified beyond FY2027.

In addition to using a portion of TSA passenger fee collections for Treasury debt reduction, statute also stipulates that the first $250 million collected each fiscal year from passenger security fees is to be deposited into an Aviation Security Capital Fund (ASCF).[21] This amount is to be set aside to reimburse airports for costs associated with acquiring and installing in-line baggage screening systems to accommodate checked baggage explosives detection equipment and for certain other airport security improvements.

Remaining fees collected, after the General Fund and ASCF amounts are deducted, are to be applied as offsetting collections against TSA annual appropriations for aviation security expenses. Historically, these fees have covered only a portion of the total costs of TSA aviation security activities. In FY2024, TSA aviation security expenses totaled roughly $9.8 billion.[22] Offsetting fee collections totaled roughly $3.5 billion, or about 35% of total TSA spending on aviation security. The amount of fees applied as offsetting collections could increase after FY2025 when the statutory requirements for specified amounts to be deposited into the Treasury General Fund expire. It is unlikely that fee collections would cover more than about 55%-60% of future TSA aviation security costs unless TSA realizes substantial cost reductions or passenger security fees were raised. Options for increasing the contribution of security fees toward TSA aviation security operating expenses may be of interest to Congress. Congress may explore options to raise fees as a way to reduce budget deficits or to make aviation security screening operations more fiscally self-sufficient, particularly if options to separate these functions from TSA's regulatory

[18] DHS, "DHS Ends Collective Bargaining for TSA's Transportation Security Officers, Enhancing Safety, Efficiency, and Organizational Agility," March 7, 2025, https://www.dhs.gov/news/2025/03/07/dhs-ends-collective-bargaining-tsas-transportation-security-officers-enhancing.

[19] Erich Wagner, "Trump Administration Outlaws Unions at TSA," *Government Executive*, March 7, 2025, https://www.govexec.com/workforce/2025/03/trump-administration-outlaws-unions-tsa/403577/?oref=ge-homepage-river.

[20] 49 U.S.C. §44940.

[21] 49 U.S.C. §44923.

[22] TSA, "Security Fees," https://www.tsa.gov/for-industry/security-fees.

responsibilities (e.g., through expansion of the SPP or creation of a separate government aviation security screening corporation) are pursued.

Explosives Screening Strategy for the Aviation Domain

Prior to the 9/11 attacks, explosives screening in the aviation domain was limited in scope and focused on selective screening of checked baggage placed on international passenger flights. Following the 9/11 attacks, ATSA mandated 100% screening of all checked baggage placed on domestic passenger flights and on international passenger flights to and from the United States.

In addition, the Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53) mandated the physical screening of all cargo placed on passenger flights. Unlike passenger and checked baggage screening, TSA does not routinely perform physical inspections of air cargo. TSA satisfies this mandate through the Certified Cargo Screening Program (CCSP). Under the program, manufacturers, warehouses, distributors, freight forwarders, and shippers carry out screening inspections using TSA-approved technologies and procedures both at airports and off-airport facilities in concert with certified supply-chain security measures and chain-of-custody standards. Internationally, TSA works with other governments, international trade organizations, and industry to assure that all U.S.-bound air cargo shipments carried aboard passenger aircraft meet the requirements of the mandate.

Additionally, TSA works with Customs and Border Protection (CBP) to carry out risk-based targeting of cargo shipments, including use of the CBP Advance Targeting System-Cargo (ATS-C), which assigns risk-based scores to inbound air cargo shipments to identify shipments of elevated risk. Originally designed to combat drug smuggling, ATS-C has evolved over the years—particularly in response to an October 2010 cargo aircraft bomb plot that originated in Yemen—to assess shipments for explosives threats or other terrorism-related activities. CBP and TSA deployed the Air Cargo Advance Screening (ACAS) system, initiated as a pilot program in 2010, under which freight forwarders and airlines voluntarily submit key data elements of cargo manifests for predeparture vetting. P.L. 115-254 required TSA to establish an air cargo security division and to review and improve the Known Shipper Program (KSP) and CCSP to enhance their effectiveness and address any identified vulnerabilities. The act also required CBP to work with TSA to establish a formal ACAS program for inbound international cargo modelled on the long-running ACAS pilot program. It directed TSA to examine the feasibility of expanding the use of computed tomography (CT) to air cargo and examine other emerging screening technologies that may enhance air cargo screening. TSA has indicated that it is evaluating these programs and technologies and considering whether further enhancements are needed to address current and emerging threats.

TSA is also evaluating whether technology advancements may provide additional or enhanced supply chain security capabilities.[23] TSA maintains a list of approved air cargo screening technologies, including a broad array of imaging and detection technologies such as explosives detection systems (EDS) machines that utilize CT and sophisticated algorithms for automatic threat detection.[24] As technology and the threat environment has evolved, TSA identifies certain equipment as "grandfathered technology" and sets expiration dates on which the older equipment must be replaced with newer, more capable systems.[25] In general, regulated entities operating

[23] TSA, *Air Cargo Security Roadmap*, December 2021, https://www.tsa.gov/sites/default/files/tsa_air_cargo_security_roadmap.pdf.

[24] TSA, *TSA Air Cargo Screening Technology List (ACSTL)*, version 12.7.1, February 7, 2025, https://www.tsa.gov/sites/default/files/non-ssi_acstl.pdf.

[25] TSA, *TSA Air Cargo Screening Technology List (ACSTL)*, version 12.7.1, February 7, 2025.

under CCSP must maintain currently approved and operable equipment using their own nonfederal funds for procurement and upkeep.

Separately, international security requirements effective since June 30, 2021, stipulate that all inbound and outbound international air cargo, whether carried on passenger or all-cargo aircraft, must be screened before being placed onboard an aircraft unless received from a TSA-approved shipper that applies acceptable security controls and/or screening protocols.[26] This update to international requirements has led TSA to revise and reform KSP and CCSP requirements to conform with established international standards for secured packing facilities.

These risk-based measures to detect threats to air cargo have not stopped terrorists from attempting to target aircraft with explosives by exploiting air cargo vulnerabilities. In 2017, individuals with ties to the Islamic State received explosive materials that had been shipped as air cargo from Turkey to Australia. The explosives were reportedly then used to assemble an improvised explosive device that was concealed in a meat mincer that was packed in checked baggage to be placed aboard an Etihad Airways flight at Sydney International Airport, Australia.[27] Another plot was uncovered in 2024 when European authorities were alerted to incendiary devices that ignited in air cargo shipments at transfer facilities in the United Kingdom and Germany. After officials in Poland arrested multiple individuals in connection with the shipments, European investigators reportedly suspected that the incendiary devices, concealed in electric massagers shipped as air cargo, were part of a sophisticated Russian-based plot to ignite fires on cargo or passenger aircraft bound for the United States and Canada.[28]

Given the focus on the threats to aviation posed by explosives, TSA has sought to acquire various explosives screening technologies. The Transportation Security Acquisition Reform Act (P.L. 113-245) required TSA to develop a five-year technology investment plan and update it on a biennial basis and mandated formal justifications and certifications that technology investments are cost-beneficial. The act also required tighter inventory controls and processes to ensure efficient utilization of procured technologies. The TSA Modernization Act (Division K of P.L. 115-254) required TSA to submit an update of the technology investment plan annually along with its budget request. The act also required TSA to establish an innovation task force to work with industry to identify, cultivate, and accelerate the development and implementation of innovative transportation security technologies.

One aim of TSA's acquisition and technology deployment strategy is improving the capability to detect concealed explosives and bomb-making components carried by airline passengers. The October 31, 2015, downing of a Russian passenger airliner departing Sharm el-Sheikh, Egypt, reportedly following the explosion of a bomb aboard the aircraft,[29] renewed concerns over capabilities to detect explosives in baggage and cargo and monitoring of airport workers with access to aircraft, particularly overseas.

In response to a 2009 attempted bombing incident aboard a Northwest Airlines flight, the Obama Administration accelerated deployment of advanced imaging technology (AIT) whole body

[26] TSA, "Air Cargo Security Options to Mitigate Costs of Compliance with International Security Requirements," 85 *Federal Register* 20234-20238, April 10, 2020.

[27] Tom Westbrook and Jonathan Barrett, "Islamic State Behind Australians' Foiled Etihad Meat-Mincer Bomb Plot: Police," Reuters, August 4, 2017, https://www.reuters.com/article/world/islamic-state-behind-australians-foiled-etihad-meat-mincer-bomb-plot-police-idUSKBN1AJ35Z/.

[28] Bojan Pancevski et al., "Russia Suspected of Plotting to Send Incendiary Devices on U.S.-Bound Planes," *Wall Street Journal*, November 4, 2024.

[29] Andrew Roth, "Russia: Terrorist Attack Brought Down Jetliner over Sinai," *Washington Post*, November 18, 2015, p. A8.

imaging devices and other technologies at passenger screening checkpoints. This deployment responded to the 9/11 Commission recommendation to improve the detection of explosives on passengers.[30] In addition to AIT, next generation screening technologies for airport screening checkpoints include advanced technology X-ray systems for screening carry-on baggage, bottled liquids scanners, cast and prosthesis imagers, shoe scanning devices, and portable explosives trace detection equipment. Since 2020, TSA has been deploying CT-based systems, similar to EDS used to screen checked baggage, at passenger screening checkpoints to scan carry-on items. TSA has procured almost 900 of these CT-based checkpoint property screening systems (CPSS) and has plans to acquire additional units to bring the total system-wide deployment to over 1,000 units.[31]

The use of AIT has raised numerous policy questions. Privacy advocates have objected to the intrusiveness of AIT, particularly when used for primary screening.[32] To allay privacy concerns, TSA has eliminated the use of human analysis of AIT images and does not store imagery. In place of human image analysts, TSA has deployed automated threat detection capabilities using automatic targeting recognition (ATR) software. Another concern about AIT centers on the potential medical risks posed by backscatter X-ray systems, but those systems are no longer in use for airport screening, and the currently used millimeter wave systems emit nonionizing millimeter waves generally considered not harmful.[33] The effectiveness of AIT and ATR has also been brought into question. In 2015, the DHS Office of Inspector General completed covert testing of passenger screening checkpoint technologies and processes and consistently found failures in technology and procedures coupled with human error that allowed prohibited items to pass into secure areas.[34] Physical pat downs to resolve AIT alarms remain controversial because of their intrusiveness and questions about the effectiveness of pat down techniques to detect concealed threat items.

The use of AIT was controversial prior to DHS's revelations of weaknesses in passenger checkpoint screening technologies and procedures. Past legislative proposals sought to prohibit the use of whole-body imaging for primary screening (for example, H.R. 2200, 111th Congress). A provision in the FAA Modernization and Reform Act of 2012 (P.L. 112-95) required TSA to ensure that AIT systems were equipped with ATR capabilities and other features to address privacy considerations. Primary screening using AIT is now commonplace at many airports, but checkpoints at some smaller airports have not been furnished with AIT equipment and other advanced checkpoint detection technologies. This may raise questions about TSA's established long-term plans to expand AIT to ensure more uniform approaches to explosives screening across all categories of airports.

Through FY2024, TSA deployed about 1,065 AIT units and updated hardware and software of fielded units to improve threat detection and increase service life. There are no available TSA plans for procurements beyond this level, although many smaller airports are not equipped with this capability.[35] TSA manages the risk of not having system-wide deployment of AIT to a large

[30] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (W. W. Norton & Co., 2004).

[31] DHS, *Transportation Security Administration Fiscal Year 2025 Congressional Justification*.

[32] For example, see American Civil Liberties Union, "ACLU Backgrounder on Body Scanners and 'Virtual Strip Searches,'" January 8, 2010.

[33] Harvard Medical School, Harvard Health Publishing, "Are Full-Body Airport Scanners Safe?," *Harvard Health Letter*, June 2011, https://www.health.harvard.edu/diseases-and-conditions/are-full-body-airport-scanners-safe.

[34] Statement of DHS Inspector General John Roth in U.S. Congress, House Committee on Oversight and Government Reform, *Concerning TSA: Security Gaps*, 114th Cong., 1st sess., November 3, 2015.

[35] DHS, *Transportation Security Administration Fiscal Year 2025 Congressional Justification*.

extent through risk-based passenger screening measures, primarily through increased use of voluntary passenger background checks under the PreCheck trusted traveler program (discussed in the next section). PreCheck expedited screening lanes are available at more than 200 U.S. commercial passenger airports.

The FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190, Title III) directed TSA to encourage private firms to develop and commercialize new transportation security technologies and establish an innovation task force to accelerate the development of innovative technologies. Although TSA has set up an innovation task force and is seeking to foster demonstrations of novel security technologies,[36] an October 2020 Government Accountability Office (GAO) performance audit found that TSA lacked effective metrics and mechanisms to integrate and evaluate private industry testing of candidate systems.[37]

The FAA Extension, Safety, and Security Act of 2016 directed DHS to conduct a review to determine whether the Transportation Security Laboratory (TSL) in Atlantic City, NJ, whose core mission is to perform research, development, and validation of explosives detection and mitigation technologies, should be managed by TSA or another DHS entity. The laboratory was originally transferred to TSA from the Federal Aviation Administration (FAA) but has been under the DHS Science and Technology Directorate (S&T) for more than a decade. The directorate operates the TSL while TSA operates its Systems Integration Facility in Arlington, VA, which is responsible for more advanced qualification testing of technologies and conducts operational testing of candidate technologies at airports to assess real-world system performance. On rare occasions, candidate technologies that fail to meet TSA criteria may be referred for independent third-party testing before TSA reevaluates their suitability. In 2020, GAO found that TSA lacked specific metrics for evaluating third-party testing protocols, which GAO considered critical to assessing whether the third-party testing concept contributes to supplier diversity and innovation objectives.[38]

Risk-Based Passenger Screening

TSA has initiated a number of risk-based screening initiatives based on intelligence-driven assessments of security risk. These include PreCheck, modified screening procedures for children aged 12 and under, and a program to expedite screening of known flight crew and cabin crew members. TSA also has developed programs for modified screening of elderly passengers.

PreCheck is modeled on CBP trusted traveler programs, including Global Entry, SENTRI, and NEXUS. Under the program, participants vetted through a background check are processed through expedited screening lanes where they can keep shoes on and keep liquids and laptops inside carry-on bags. As of December 2024, PreCheck expedited screening lanes were available at more than 200 airports. The cost of background checks under the PreCheck program is recovered through initial application fees for a five-year membership ranging from $76.75 to $85 per passenger and renewal fees ranging from $58.75 to $70 for online renewals or $66.75 to $77.95 for in-person renewals.[39]

[36] See TSA, "Innovation Task Force," https://www.tsa.gov/itf.

[37] Government Accountability Office (GAO), *TSA Acquisitions: TSA Needs to Establish Metrics and Evaluate Third Party Testing Outcomes for Screening Technologies*, GAO-21-50, October 2020, https://www.gao.gov/assets/720/710403.pdf.

[38] GAO, *TSA Acquisitions*, GAO-21-50.

[39] TSA, "TSA PreCheck," https://www.tsa.gov/precheck.

Although it is unclear whether PreCheck is fully effective in directing security resources to unknown or elevated-risk travelers, it has improved screening efficiency. In 2016, TSA estimated annual savings in direct screener workforce costs of $110 million as a result of PreCheck and other risk-based initiatives.[40] A 2017 study suggested that considerably greater efficiency gains might be realized if TSA could double the annual number of PreCheck screenings, which would require increasing the number of PreCheck-eligible travelers to about 15-20 million.[41]

P.L. 115-254 directed TSA to work with at least two private sector entities to expand PreCheck enrollment options and set an enrollment target of 15 million by the end of FY2021. Currently, TSA partners with three enrollment vendors—Telos, Clear, and Idemia—to collectively offer over 900 enrollment locations. According to TSA, PreCheck enrollment surpassed 20 million active members as of August 2024.[42] In addition, participants in CBP trusted traveler programs—including Global Entry and, in some cases, NEXUS and SENTRI—are eligible to use PreCheck screening lanes, bringing the total number of vetted air travelers under DHS trusted traveler programs to over 40 million.

P.L. 115-254 also required TSA to ensure that PreCheck expedited screening lanes are open and available to program participants during peak and high-volume travel times and directed TSA to take steps to provide expedited screening at standard screening lanes when PreCheck lanes are unavailable. It also instructed TSA to ensure that only trusted traveler program members and members of the Armed Forces are permitted to use PreCheck screening lanes.

The act also directed TSA and CBP to work together on the deployment of biometric technologies for the entry-exit program for international travelers and other uses. According to the *TSA Identity Management Roadmap*,[43] TSA plans to continue its efforts to integrate biometrics technology for identity verification of PreCheck travelers and potentially further scale the use of biometrics to all domestic air travelers through voluntary opt-in practices. Plans for increased use of biometrics may raise privacy and data protection concerns that might be of interest to Congress.

The Registered Traveler program was a predecessor test program to PreCheck. The program used private vendors to issue and scan participants' biometric credentials but was scrapped by TSA in 2009 because it failed to show a demonstrable security benefit. In 2016, biometric identity authentication was reintroduced at 13 airports under a private trusted traveler program known as Clear. Clear is now available in more than 55 airports.[44] Participants in Clear, which is separate from PreCheck and not operated or funded by TSA, use an express lane to verify identity using their fingerprint or iris scan rather than interacting with a TSA document checker.[45] While Clear does not directly address or improve aviation security programs, it offers airline passengers the option to pay membership fees for potential time-saving convenience.

TSA has worked with CBP to deploy facial recognition technology (FRT) for verifying PreCheck program participants at expedited screening lanes using CBP's traveler verification service

[40] TSA, *Congressional Budget Justification FY2016,* Aviation Security, p. 5.

[41] Sheldon H. Jacobson et al., "When Should TSA PreCheck Be Offered at No Cost to Travelers?," *Journal of Transportation Security*, vol. 10, June 2017, pp. 23-39.

[42] TSA, "TSA PreCheck Reaches Milestone with 20 Million Members," press release, August 8, 2024, https://www.tsa.gov/news/press/releases/2024/08/08/tsa-precheckr-reaches-milestone-20-million-members.

[43] TSA, *TSA Identity Management Roadmap*, February 2022, https://www.tsa.gov/sites/default/files/tsa_idm_roadmap_2022-03-01_508c_final.pdf.

[44] CLEAR, "CLEAR Locations: Discover CLEAR Near You," https://www.clearme.com/where-to-use-clear?service-types=clear-plus.

[45] Scott McCartney, "The Airport Security Shortcut That Isn't PreCheck," *Wall Street Journal*, June 22, 2016, http://www.wsj.com/articles/the-airport-security-short-cut-that-isnt-precheck-1466616335.

(TVS). TVS uses FRT to match live captured photos of travelers to DHS databases. Air travelers may also be scanned using FRT and the TVS on international flights, particularly international arrivals during CBP customs screening.

TSA has also deployed FRT as a means to voluntarily match air travelers to their identification documents.[46] TSA has deployed second generation credential authentication (CAT-2) systems and has upgraded older CAT systems with facial image capture capabilities at airport passenger screening checkpoints. Through FY2024, TSA procured about 1,800 upgrade kits and almost 200 new CAT-2 units, making these FRT capabilities available at most airport checkpoints. In addition to scanning boarding passes and traveler identification documents, these systems can capture traveler images and use FRT for identity verification purposes. Concerns have been raised that travelers may not always be aware that identity verification using FRT is currently voluntary. TSA has indicated that it is updating signage at document checker kiosks to clarify that passengers may decline to be photographed by these systems. In the 118th Congress, a number of bills were considered that would have placed curbs or limits on further expansion of the use of FRT in a broad array of settings. In addition, an amendment to the 2025 DHS Appropriations Act (H.Amdt. 1011) that would have eliminated funding to further expand TSA's use of FRT was agreed to in the House by a voice vote.

While use of FRT for passenger identity verification remains voluntary and controversial, TSA implemented a requirement for passengers to use identification compliant with Real ID standards, effective as of May 7, 2025.[47] The requirements, set forth in the Real ID Act of 2005 (P.L. 109-13, Division B), establish standards for driver's licenses and other state-issued personal identification cards that are acceptable forms of identification to present to federal agencies (e.g., TSA) for official purposes, such as accessing federally regulated airports and commercial aircraft. Although all U.S. states, the District of Columbia, and all five U.S. territories have developed Real ID compliant identification documents, not all identification cards currently in use by individuals meet Real ID standards, and noncompliant cards will no longer be accepted at TSA passenger screening checkpoints. Currently, five states (Michigan, Minnesota, New York, Vermont, and Washington) issue enhanced driver's licenses and identification cards usable for land-border crossings that are also considered acceptable alternatives to Real ID for accessing TSA checkpoints and federal facilities. TSA may refuse passengers without Real ID compliant cards or acceptable alternatives. This may cause travel disruptions and delays at screening checkpoints. TSA implementation and enforcement of Real ID requirements may be a topic of interest in the 119th Congress.

In addition to passenger screening, TSA, in coordination with participating airlines and labor organizations representing airline pilots, has developed a known crewmember program to expedite security screening of airline flight crews.[48] In July 2012, TSA expanded the program to include flight attendants.[49] TSA has announced that, in coordination with vendor NATA Compliance Services, the known crewmember program will be replaced by the Crewmember Access Point system and expects that this transition will occur in late November 2025.[50]

[46] TSA, "Facial Recognition Technology," https://www.tsa.gov/news/press/factsheets/facial-recognition-technology.

[47] See DHS, "REAL ID," https://www.dhs.gov/real-id.

[48] See Known Crewmember, http://www.knowncrewmember.org/.

[49] Hugo Martin, "TSA To Allow Flight Attendants to Use Faster Security Line," *Los Angeles Times*, July 23, 2012, https://www.latimes.com/business/la-xpm-2012-jul-23-la-fi-mo-flight-attendants-faster-security-line-20120723-story.html.

[50] NATA Compliance Services, AIRTERA, "Crewmember Access Point (CMAP)," https://info.natacs.aero/crewmember-access-point-faq.

TSA has also developed a passenger behavior detection program to identify potential threats based on observed behavioral characteristics. TSA initiated early tests of its Screening Passengers by Observational Techniques program in 2003. By FY2012, the program deployed almost 3,000 behavior detection officers at 176 airports at an annual cost of about $200 million. The effectiveness of the behavioral detection program is unclear, and privacy advocates have cautioned that it could devolve into racial or ethnic profiling. While some Members of Congress have sought to shutter the program, the 118th and earlier Congresses did not move to do so. The 118th and earlier Congresses also did not take specific action to revamp the program, although both GAO and the DHS Office of Inspector General had raised concerns about the program's effectiveness.[51] Scrutiny of the program prompted TSA to reportedly revamp and relabel it as the Behavior Detection and Analysis program, largely based on a 2018 DHS S&T-sponsored study of behavioral assessment techniques using visual observation to enhance the selection and training of behavior detection officers.[52]

P.L. 115-254 directed TSA to utilize risk-based strategies in deploying federal air marshal teams on international and domestic flights. Air marshals are deployed under risk-based scheduling practices and must meet statutory obligations to cover all flights that are assessed as high-risk.[53] A different TSA initiative used air marshals to shadow passengers whose behavioral profiles included past international travel to certain countries and regions that triggered elevated security risk determinations. The program was reportedly shuttered in December 2018 after media reports and some Members of Congress raised concerns over its privacy implications.[54] TSA still utilizes passenger travel data to develop temporary watch lists that are used in conjunction with permanent terrorist watch lists as screening tools to identify high-risk passengers who are subject to enhanced screening before boarding a flight.[55]

The Use of Terrorist Watch Lists in the Aviation Domain

Airlines had been responsible for checking passenger names against terrorist watch lists maintained by the government before the Intelligence Reform and Terrorist Prevention Act of 2004 (P.L. 108-458) mandated that DHS assume this function. Efforts to transfer this responsibility to DHS were delayed by concerns regarding privacy and data protections. Following at least two separate instances in 2009 and 2010 in which passenger record checks failed to identify individuals who might have posed a threat to aviation, TSA took responsibility for checking passenger names under the Secure Flight program. In November 2010, DHS announced that 100% of passengers flying to or from U.S. airports were being vetted using the Secure Flight system.[56] According to TSA, it has maintained its target of vetting 100% of airline

[51] GAO, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013; DHS, Office of Inspector General, *Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)*, OIG-13-91, May 29, 2013; and Statement of DHS Deputy Inspector General Charles K. Edwards in U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security, *TSA's SPOT Program and Initial Lessons From the LAX Shooting*, 113th Cong., 1st sess., November 13, 2013.

[52] RTI International, *Behavior Detection Visual Search Task Analysis Project: Visual Search Battery Report*, May 2018, https://www.dhs.gov/publication/st-behavior-detection-visual-search-task-analysis-project-visual-search-battery-report.

[53] See 49 U.S.C. §44917.

[54] Jana Winter and Jenn Abelson, "TSA Says It No Longer Tracks Regular Travelers as if They May Be Terrorists," *Boston Globe*, December 15, 2018.

[55] DHS, *Privacy Impact Assessment Update for Secure Flight: Silent Partner and Quiet Skies*, DHS/TSA/PIA-018(i), April 19, 2019, https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

[56] DHS, "DHS Now Vetting 100 Percent of Passengers on Flights Within or Bound for U.S. Against Watchlists," press release, November 30, 2010.

passengers, as well as non-travelers seeking access to sterile areas of airport concourses, against high-risk watch lists. It also vets all passengers boarding U.S.-bound flights from foreign last point of departure airports and passengers onboard flights that fly through U.S. airspace but do not land at a U.S. airport. In FY2023, TSA vetted almost 1.3 billion submissions.[57]

Secure Flight vets passenger name records against a subset of the Terrorist Screening Database (TSDB). On international flights, Secure Flight also compares passenger records with watch lists compiled by CBP's National Targeting Center (Passenger Division), which relies on the Advance Passenger Information System and other tools to vet both inbound and outbound passenger manifests. In addition to flights of U.S. and foreign airlines, all inbound and outbound international flights using chartered and private aircraft must transmit passenger and crew manifests to CBP at least one hour prior to departure.

In addition to these systems, TSA conducts risk-based analysis of passenger data through the Secure Flight system to determine whether passengers are to be denied boarding or receive expedited, standard, or enhanced screening at airport checkpoints.[58] Secure Flight compares passenger records against the No-Fly and Selectee lists, which are subsets of the TSDB used to identify individuals that are to be denied boarding or that must undergo enhanced security screening. Individuals on the No-Fly List are to be denied boarding and referred to law enforcement authorities. In addition to the No-Fly List, TSA maintains a list of individuals, referred to as the Selectee List or Automatic Selectee List, who are to be automatically selected for enhanced pre-flight screening. Enhanced screening includes a more thorough examination of carry-on bags and checked baggage and, in some instances, pat-downs and the use of chemical trace detection swabs to test for explosives residue. Passengers not on these lists can be randomly selected for enhanced screening, and passengers or baggage that trigger alarms during initial screening may undergo these additional measures.

In addition, there has been a growing interest in finding better ways to utilize watch lists to prevent terrorist travel, particularly travel of radicalized individuals seeking to join forces with foreign terrorist organizations. Central issues surrounding the use of terrorist watch lists in the aviation domain that may be considered by the 119th Congress include

- the speed at which watch lists are updated as new intelligence information becomes available;
- the extent to which all information available to the federal government is exploited to assess possible threats among passengers and airline and airport workers;
- the ability to detect identity fraud or other attempts to circumvent terrorist watch list checks;
- the adequacy of established protocols for providing redress to individuals improperly identified as potential threats; and
- the adequacy of coordination with international partners.[59]

Following the January 6, 2021, security breach of the U.S. Capitol, policy debate ensued regarding potential inclusion of U.S. citizens and permanent residents who have engaged in

[57] DHS, *Transportation Security Administration Budget Overview: Fiscal Year 2025 Congressional Justification*.

[58] TSA, "Privacy Act of 1974; Department of Homeland Security Transportation Security Administration-DHS/TSA-019 Secure Flight Records System of Records," 80 *Federal Register* 233-239, January 5, 2015.

[59] For additional information, see CRS Report RL33645, *Terrorist Watchlist Checks and Air Passenger Prescreening*, by William J. Krouse and Bart Elias (available to congressional clients on request).

domestic terrorism or anti-government violence on the No-Fly List.[60] Additionally, past airline actions to ban disruptive passengers (including passengers who refused to comply with onboard masking requirements during the COVID-19 pandemic) have prompted debate about the desirability of replacing airlines' "blacklists," which are not shared with other air carriers or the government, with centralized lists of disruptive passengers. FAA has asserted its authority to impose stiff civil penalties and pursue possible criminal charges against passengers who interfere with or fail to comply with directions from airline crewmembers but has not addressed barring such individuals from future air travel.

Historically, the TSA lists and the broader TSDB have focused on international terrorist threats. Their possible use for the additional purposes discussed above may prompt congressional debate about whether an expansion of watch lists could divert TSA from its traditional focus.

Perimeter Security, Access Controls, and Worker Vetting

Airport operators generally are responsible for airport perimeter security, access controls, and airport worker credentialing. There is no common access credential for airport workers; rather, each airport separately issues security credentials to airport workers. These credentials are often referred to as Security Identification Display Area (SIDA) badges, and they convey the level of access that an airport worker is granted. TSA regulates and oversees compliance with airport badging and access control requirements.

TSA requires access control points to be secured by measures such as posted security guards or electronically controlled locks. Additionally, airports must implement programs to train airport workers to challenge anyone not displaying proper identification in secure areas.[61]

TSA requires security background checks of airport workers who are granted unescorted access privileges to secure areas at all commercial passenger airports and air cargo facilities. Background checks consist of a fingerprint-based criminal history records check and security threat assessment, which includes checking employee names against terrorist database information. Certain criminal offenses committed within the past 10 years, including aviation-specific crimes, transportation-related crimes, and other felony offenses, are disqualifying. Airports must collect an applicant's biographical information and fingerprints and submit these data to TSA to process background checks.

P.L. 115-254 established more stringent standards for individuals applying for SIDA access in order to strengthen vetting effectiveness (e.g., requiring that such individuals also provide their social security number). Many airports coordinate with a service known as the Transportation Security Clearinghouse to process background check applications.[62] In addition to initial background checks that examine criminal histories over the past 15 years, TSA conducts recurrent vetting of airport workers with SIDA access credentials using the Federal Bureau of Investigation's Rap Back service.[63] TSA also maintains a centralized database of individuals who have had security access or aircraft-operator credentials revoked for failing to comply with statutory aviation security requirements.

TSA also conducts random physical inspections of airport workers at SIDA access points and in SIDA areas. P.L. 115-254 clarified that TSA-led random inspections of aviation workers must be

[60] See CRS In Focus IF11731, *Aviation Security Measures and Domestic Terrorism Threats*, by Bart Elias.

[61] See 49 C.F.R. §1542.211(d).

[62] See American Association of Airport Executives, "Transportation Security Clearinghouse," https://aaae.org/tsc.

[63] DHS, *Airport Access for Aviation Workers*, DHS/TSA/PIA-020(c), April 27, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa020c-airportaccessaviationworkers-april2020.pdf.

targeted, strategic, and focused on providing the greatest level of security effectiveness rather than being "random" in the true sense of the word. The law also directed TSA to continue its covert testing of employee access controls and provide measures of the effectiveness of such operations to airport operators and, as appropriate, to airlines.

Airports may also deploy surveillance technologies, access control measures, and security patrols to protect airport property, including buildings and terminal areas, from intrusion. Such measures are paid for by the airport but must be approved by TSA as part of an airport's overall security program. In coordination with airport security, state and local law enforcement agencies that have jurisdiction over airports are generally responsible for patrols of airport property, including passenger terminals. They also may patrol adjacent properties to deter and detect other threats to aviation, such as shoulder-fired missiles (see "Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft").

Explosives Screening Technology and Canines

Explosives screening technologies at passenger checkpoints primarily consist of the AIT whole body imaging systems, advanced technology X-ray imagers for carry-on items, and explosives trace detection systems used to test swab samples collected from individuals or carry-on items for explosives residue (see "Explosives Screening Strategy for the Aviation Domain"). TSA introduced CT scanning technology at passenger checkpoints in FY2018. P.L. 115-254 directed TSA to proceed with the use of CT to screen both carry-on items and cargo loaded on passenger aircraft. The act also directed TSA to assess other emerging screening technologies that may be used to enhance air cargo screening. Through FY2023, TSA had deployed about 780 units at airports across the United States. TSA asserts that CT technology offers automated capabilities to help improve detection of explosives and other threats.[64]

For checked baggage screening, TSA utilizes a combination of CT-based EDS and chemical trace detection technology. TSA deploys high-speed (greater than 900 bags per hour), medium-speed (400-900 bags per hour), or reduced-speed (100-400 bags per hour) CT-based systems, depending on airport needs and configurations. TSA is also funding the development of new algorithms to detect homemade explosives threats in checked baggage and reduce false positives. TSA may reimburse airports for modifying baggage handling facilities and installing new inspection systems to accommodate explosives detection technologies.

In addition to detection technologies, TSA also utilizes explosives detection canine teams to meet screening mandates. TSA's National Explosives Detection Canine Team Program trains and deploys canines and their handlers at transportation facilities to detect explosives. The program includes approximately 420 TSA teams and 675 state and local law enforcement teams trained by TSA under partnership agreements. The TSA teams are dedicated to passenger screening at 47 airports; just over 500 of the state and local law enforcement teams work in aviation, mostly focusing on air cargo.

P.L. 115-254 directed TSA to establish a working group to assess ways to support a decentralized, nonfederal domestic breeding program for explosives detection canines and to modernize canine breeding, medical, technical, and training standards. It further instructed TSA to develop guidance for the procurement and deployment of third-party domestic canines to enhance public area security at transportation hubs, including airports. Large hub airports are permitted to directly acquire canines from TSA-approved third-party sources, so long as canines procured in this

[64] DHS, *Transportation Security Administration Budget Overview: Fiscal Year 2019 Congressional Justification*, https://www.dhs.gov/sites/default/files/publications/Transportation%20Security%20Administration.pdf.

manner were trained by TSA personnel. Additionally, the act directed TSA to issue standards for the primary screening of air cargo by private entities using dogs and handlers not owned or employed by TSA. TSA began approving third-party canine teams in late 2018 for air cargo screening and explosives detection in airport terminals. The 119th Congress may have an interest in oversight of the third-party canine program, including reviewing its use and effectiveness in screening air cargo and patrolling airport terminals.

Protecting Public Areas of Airports

Incident response at airports is primarily the responsibility of airport operators and state or local law enforcement agencies, with TSA acting as a regulator in approving an airport's comprehensive security program. Federal law enforcement may also be involved in developing and reviewing response plans but typically does not have a lead role in event response; however, it may assume a lead investigative role following a security incident, particularly if the event is determined to be an act of terrorism. For example, on November 1, 2013, a lone gunman targeting TSA employees fired several shots at a screening checkpoint in Los Angeles International Airport (LAX), killing one TSA screener and injuring two other screeners and one airline passenger. In a detailed post-incident action report, TSA identified several proposed actions to improve checkpoint security but did not support proposals to arm certain TSA employees or provide screeners with bulletproof vests and did not recommend mandatory law enforcement presence at checkpoints.

The Gerardo Hernandez Airport Security Act of 2015 (P.L. 114-50), enacted in September 2015, was named in honor of the TSA screener killed in the LAX incident. The act required airports to adopt plans for responding to security incidents and to create a mechanism for sharing information among airports regarding best practices for airport security incident planning, management, and training. It also required TSA to identify ways to expand the availability of funding for checkpoint screening law enforcement support through cost savings from improved efficiencies mainly achieved through implementing PreCheck expedited screening protocols. TSA partially reimburses local law enforcement agencies for support at screening checkpoints, and P.L. 115-254 directed TSA to increase funding for the reimbursable program to expand protection of public areas of airports and screening checkpoints. It also directed TSA to establish a working group to collaborate with public and private stakeholders to develop nonbinding recommendations for enhancing security in public areas of transportation facilities.

In October 2019, TSA published the working group's findings regarding best practices and recommendations for protecting public areas that highlighted the role of airport law enforcement and the benefits of visible deterrence provided through law enforcement presence supported through TSA's law enforcement reimbursable program.[65] TSA, however, continued to advocate for eliminating law enforcement reimbursable agreements, noting that while the number of airports in the program has grown in recent years, funding has remained flat at about $45 million annually, resulting in decreases in reimbursements per participant. In FY2024, TSA eliminated the law enforcement reimbursement program, as well as the canine reimbursement program for non-TSA canine teams that engage in explosives detection and deterrence at airports. In its FY2025 budget, TSA repeated its long-standing request to also eliminate funding for exit lane staffing by TSA screening personnel. Such action would require a change in statute, which currently mandates that TSA provide for the monitoring of passenger exit points from the sterile

[65] TSA, *Protecting Public Areas: Best Practices and Recommendations*, October 2019, https://www.tsa.gov/sites/default/files/documents/hr302.section_1931.best_practices_9-25-19_3_oct17_final.pdf.

area of airports.[66] TSA has long regarded exit lane staffing, which costs in excess of $100 million per year, as an airport responsibility though the mandate assigns this responsibility to TSA.[67] Moreover, TSA asserts that deployment of various physical barriers, such as interlocking doors and multilayered portals as well as video and sensor technologies, deployed at exits can help reduce staffing needs.[68] The status of funding for these airport security measures and TSA's role in supporting these efforts may be of interest to the 119th Congress during appropriations debates.

On January 17, 2017, a mass shooting killing five people in a baggage claim area of the Fort Lauderdale-Hollywood International Airport in Florida was perpetrated by an arriving passenger who had properly declared the handgun and two magazines used in the attack and had transported them in a locked box as required by federal regulations. In general, airline passengers are not prohibited from transporting firearms aboard aircraft so long as the firearms are transported unloaded and locked as checked baggage. In mid-January 2021, some airlines temporarily prohibited passengers from checking firearms on flights to the Washington, DC, area due to concerns that individuals might travel to the area to engage in armed protests and demonstrations. The 119th Congress may consider whether such policies and actions may continue to fall to individual airlines and whether they may raise constitutional issues.

Foreign Last Point of Departure Airports

TSA regulates foreign air carriers that operate flights to the United States to enforce requirements regarding the acceptance and screening of passengers, baggage, and cargo carried on those aircraft.[69] Under these regulations, TSA inspects foreign airports from which commercial flights proceed directly to the United States. TSA representatives (TSARs) oversee assessments of country compliance with international standards for aviation security and plan and coordinate risk assessments of foreign airports. TSARs also administer and coordinate TSA responses to terrorist incidents and threats to U.S. citizens and transportation assets and interests overseas.

Fifteen foreign last point of departure airports in six countries have CBP preclearance facilities where passengers are admitted to the United States prior to departure.[70] Passengers arriving on international flights from these preclearance airports deplane directly into the U.S. arrival airport's sterile area, where they can board connecting flights or leave the airport directly rather than being routed to customs and immigration processing facilities. Although CBP has announced its intention to expand customs preclearance to additional countries, no additional preclearance locations have been established.[71] CBP is also working to implement international remote

[66] 49 U.S.C. §44903(n).

[67] Bart Jansen, "Airport Execs Clash with TSA Over Dropping Exit Lanes," *USA Today,* November 5, 2013, https://www.usatoday.com/story/travel/flights/2013/11/05/tsa-airports-exit-lanes/3435877/; and Kylie Bielby, "Pekoske Outlines TSA Budget Request for Screening and Authentication Technologies," *PT World, Passenger Terminal Today,* April 24, 2024, https://www.passengerterminaltoday.com/news/security/pekoske-outlines-tsa-budget-request-for-screening-and-authentication-technologies.html.

[68] TSA, *Exit Land Staffing, Fiscal Year 2023*, June 30, 2023, https://www.dhs.gov/sites/default/files/2023-08/23_0630_tsa_exit_lane_staffing_fy23.pdf.

[69] See 49 C.F.R. Part 1546.

[70] U.S. Customs and Border Protection (CBP), "Preclearance," https://www.cbp.gov/travel/preclearance.

[71] CBP, "Preclearance Expansion" https://www.cbp.gov/travel/preclearance/preclearance-expansion#:~:text=Building%20upon%20the%20success%20of%20existing%20Preclearance%20operations%2C,submit%20inquiries%20pertaining%20to%20Preclearance%20expansion%20to%20preclearance.expansion%40cbp.dhs.gov.

baggage screening in coordination with foreign partners so checked bags do not have to be claimed at the U.S. airport of entry, which has been the practice.[72]

P.L. 114-190 requires TSA to conduct security risk assessments at all last point of departure airports and authorizes the donation of security screening equipment to such foreign airports to mitigate security vulnerabilities that put U.S. citizens at risk. P.L. 115-254 mandated that any such donated screening equipment be restored to original commercial settings and must not contain TSA-specific security standards or algorithms. Recipients of donated screening equipment must demonstrate that they can properly maintain it and must ensure that once the equipment is retired from service, it does not get into the hands of terrorists or otherwise compromise security.

P.L. 115-254 also directed TSA to work with FAA to track public charter flights between the United States and Cuba and assess aviation security measures at Cuban airports that have air service to the United States. The United States restricted scheduled air service and public charter flights between the United States and airports in Cuba other than José Martí International Airport due to international policy concerns during the first Trump Administration.[73] In 2022, during the Biden Administration, the United States relaxed some of these restrictions, allowing limited scheduled flights and group charters between the United States and Cuba to resume.[74] Cuba is the only country designated as a State Sponsor of Terrorism that has direct flights to the United States.[75]

Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft

The terrorist threat posed by small, man-portable, shoulder-fired missiles was brought into the spotlight by the November 2002 attempted downing of a chartered Israeli airliner in Mombasa, Kenya. Since then, Department of State and military initiatives have sought bilateral cooperation and voluntary reductions of shoulder-fired missiles, formally referred to as man-portable air defense systems (MANPADS), worldwide.

The most visible DHS initiative to address this threat was the multiyear Counter-MANPADS program carried out by DHS S&T. The program concluded in 2009 with extensive testing and FAA certification of two systems capable of protecting airliners against heat-seeking missiles. The systems have not been deployed on commercial airliners in the United States largely because of high acquisition and life-cycle costs. U.S. airlines have not voluntarily invested in these systems for operational use.

MANPADS are seen as a security threat to civil aviation overseas. A MANPADS attack, particularly one within the United States, could considerably impact the airline industry. Major

[72] CBP, "CBP Launches Innovative International Remote Baggage Screening Initiative to Enhance Security and Streamline Travel," April 8, 2025, https://www.cbp.gov/newsroom/national-media-release/cbp-launches-innovative-international-remote-baggage-screening.

[73] U.S. Department of State, Office of the Spokesperson, "United States Restricts Scheduled Air Service to Cuban Airports," October 25, 2019, https://2017-2021.state.gov/united-states-restricts-scheduled-air-service-to-cuban-airports/ ; and Michael R. Pompeo, Secretary of State, "Press Statement: United States Further Restricts Air Travel to Cuba," January 10, 2020, https://2017-2021.state.gov/united-states-further-restricts-air-travel-to-cuba/.

[74] Hannah Sampson, "Biden's Revised Cuba Policy Creates More Options for U.S. Travelers," *Washington Post*, June 2, 2022, https://www.washingtonpost.com/travel/2022/06/02/new-cuba-policy-travel-americans/.

[75] Testimony of TSA Executive Assistant Administrator for Security Operations Melanie Harvey and TSA Executive Assistant Administrator for Operations Support Stacey Fitzmaurice in U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, *Protecting the Homeland – Examining TSA's Relationships with U.S. Adversaries*, 118th Cong., 2nd sess., July 9, 2024.

U.S. airports have conducted vulnerability studies, but efforts to reduce vulnerabilities to potential MANPADS attacks face operational challenges given the extensive area around airports where airplanes flying at low altitudes are vulnerable to shoulder-fired missile attacks. While Congress has not formally debated the issue since the conclusion of the Counter-MANPADS program in 2009, any future terrorist attempts to use a shoulder-fired missile or similar armament to attack civilian aircraft, including airliners chartered to transport U.S. servicemembers, could escalate this topic to a national security priority.

Security Issues Regarding the Operation of Unmanned Aircraft

The proliferation of civilian drones, also known as unmanned aircraft systems (UAS), raises potential security risks, including the possibility that terrorists could use a drone to carry out an attack against a ground target. It is also possible that drones themselves could be targeted by terrorists or cybercriminals seeking to tap into sensor data transmissions or cause mayhem by hacking or jamming command and control signals. Two principal concerns are that drones could be used to attack critical infrastructure or high-profile targets and that unauthorized drone operations in close proximity to airports could disrupt air transportation. The 119th Congress may have an interest in policies and technologies to mitigate safety and security threats posed by UAS.

Terrorists could use drones to carry out small-scale attacks using explosives or as platforms for chemical, biological, or radiological attacks. In addition, drone flights near major airports have disrupted commercial aviation when no weapon was involved. Domestically, there have been numerous reports of drones flying in close proximity to airports and manned aircraft, in restricted airspace, and over stadiums and outdoor events. In December 2024, numerous drone sightings in the Northeast, mostly over New Jersey, were logged with state and local police and federal authorities, prompting congressional hearings.[76]

In some cases, drones have collided with manned aircraft. For example, in September 2017, a hobby drone collided with a National Guard Black Hawk helicopter assigned to patrol the skies over New York harbor during a meeting of the UN General Assembly, causing damage to one of the helicopter's rotor blades. Similarly, in January 2025, a small drone collided with a firefighting tanker conducting aerial fire suppression operations over a wildfire in Los Angeles, CA.[77]

Numerous other safety incidents involving drones have been reported in the United States and abroad; few have been tied to terrorism. The Islamic State is known to have used small drones in conflict zones to conduct reconnaissance and drop explosives. Militarized small drones have played a role in the Russia-Ukraine war for both reconnaissance and tactical strikes, demonstrating their potential capabilities and the extent of their threat if deployed by a terrorist organization. The limited payload capacities of small unmanned aircraft would likely limit the damage they could inflict if loaded with conventional explosives, but a drone attack using chemical, biological, or radiological weapons could have a more widespread impact.

Regulations for small unmanned aircraft used for commercial purposes require TSA to carry out security threat assessments of certificated operators as it does for civilian pilots.[78] This requirement does not apply to recreational UAS users, who are generally permitted to operate small drones at low altitudes. FAA has issued guidance to law enforcement regarding unlawful

[76] See CRS Insight IN12476, *Drone Encounters Prompt Calls for Restrictions and Other Protections*, by Bart Elias.

[77] Jaimie Ding and Olga R. Rodriquez, "Man Agrees to Plead Guilty for Flying Drone That Damaged Firefighting Aircraft in LA Wildfire," Associated Press, January 31,2025 https://apnews.com/article/california-wildfires-los-angeles-guilty-drone-8406f5ed22b73bd597fc6978eba54dc9.

[78] See 14 C.F.R. §61.18.

UAS operations,[79] but it is unclear whether state and local law enforcement agencies, which often are first to respond to drone incidents, have sufficient training or technical capacity to respond to potential threats.[80]

Technology may help manage security threats posed by unmanned aircraft. Integrating tracking mechanisms and incorporating "geofencing" capabilities, designed to prevent flights over sensitive locations or in excess of certain altitude limits, into UAS may help curtail unauthorized flights.[81] It was reported in January 2025 that after previously integrating geofencing capabilities on its drones for about a decade, Chinese drone manufacturer DJI, which controls about 70% of the civilian drone market in the United States, had chosen to make use of these features optional on its drones. There is no federal law or regulation requiring geofencing technology on drones.

FAA regulations generally require most nonmilitary drones to broadcast position information and a unique identifier, referred to as "remote ID." In January 2021, FAA issued regulations requiring drones to be equipped with remote ID capabilities that continually broadcast position and identification information. This can be accomplished through built-in capabilities generally required for drones manufactured since September 2022 via remote ID modules affixed to drones without built-in capabilities or by operating within the confines of an FAA-recognized identification area, such as an airpark designated for remote-controlled model aircraft.[82]

Language in the FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) directed FAA to establish an application process for owners and operators of critical infrastructure sites and amusement parks to request that FAA designate surrounding airspace as off-limits to drones.[83] The FAA Reauthorization Act of 2024 (P.L. 118-63) added state prisons to the list of sites eligible to apply for these drone restrictions. FAA has not established the process for designating such sites as drone-restricted areas.

The National Defense Authorization Act for FY2017 (P.L. 114-328) authorized the Armed Forces and the Department of Energy to take necessary actions to mitigate threats posed by UAS to certain security-related facilities in the United States. The act authorizes the military to detect, monitor, and track UAS; issue warnings to operators; disrupt control of UAS, including interrupting or jamming control signals; seize or take control of UAS; confiscate UAS; or use reasonable force to disable or destroy UAS. The statute has since been expanded to include additional military facilities and missions.[84]

P.L. 115-254 authorized the Department of Justice and DHS to take similar actions to protect people, facilities, or assets from credible threats posed by UAS. These authorities have been extended multiple times, most recently in the FY2025 full-year continuing resolution (H.R. 1968), which keeps them in effect until September 30, 2025. P.L. 115-254 also expanded the mission of the Coast Guard to include carrying out protective measures to safeguard its facilities and assets, including Coast Guard vessels and aircraft, from threats posed by UAS. P.L. 115-254

[79] Federal Aviation Administration (FAA), *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*, https://www.faa.gov/uas/resources/policy_library/media/FAA_UAS-PO_LEA_Guidance.pdf.

[80] Statement of International Association of Chiefs of Police President Chief Richard Beary in U.S. Congress, House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, *Unmanned Aerial System Threats: Exploring Security Implications and Mitigation*, 114th Cong., 1st sess., H.Hrg. 114-9, March 18, 2015.

[81] For example, see Todd Humphreys, *Statement on the Security Threat Posed by Unmanned Aerial Systems and Possible Countermeasures*, submitted to House Committee on Homeland Security, Subcommittee on Oversight and Management Efficiency, 114th Cong., 1st sess., March 16, 2015.

[82] FAA, "Remote Identification of Unmanned Aircraft," 86 *Federal Register* 4390-4513, January 15, 2021.

[83] P.L. 114-190, §2209.

[84] 10 U.S.C. §103i.

directed FAA and DOT to coordinate with the various agencies authorized to engage in counter-unmanned aircraft systems (C-UAS) activities and work with the agencies to ensure technologies developed to mitigate risks posed by errant or hostile UAS do not adversely impact safe airport and air traffic operations.

P.L. 115-254 also established a formal prohibition against civilians who arm unmanned aircraft with dangerous weapons. Additionally, the act established criminal penalties for flying a drone over the White House grounds, the Vice President's residence, sites where the President or other individuals protected by the Secret Service are visiting, and other buildings or grounds hosting a special event of national significance. It also established criminal penalties for using a drone in a manner that interferes with wildfire suppression efforts or related law enforcement or emergency response activities.

During the 118th Congress, several bills were considered that would have expanded options for detecting and interdicting drones; none of these proposals were enacted.[85] In light of the recent attention on this issue, the 119th Congress may have an interest in reviewing the adequacy and effectiveness of existing statutes pertaining to drone uses that pose a security risk and the legal framework for C-UAS measures to detect and interdict such operations.

Transit and Passenger Rail Security[86]

Bombings of and shootings on passenger trains in Europe and Asia illustrate the vulnerability of passenger rail systems to terrorist attacks. Public transit systems in the United States annually carry about eight times as many passengers as airlines do. According to the Federal Transit Administration, in 2023, there were 6.9 billion unlinked passenger trips via public transit and 29 million unlinked passenger trips via intercity rail,[87] compared with 819 million enplanements via aviation.[88] The increased efforts around air travel security have led to concerns that terrorists may turn their attention to other targets, such as transit or passenger rail. Congress may consider weighing options for increased rail passenger security with such concerns as the efficient functioning of transit systems and the potential costs and damages of an attack.

Nearly 6,800 organizations provide public transportation in the United States.[89] As there are over seven times as many buses available for service than passenger railcars, the challenge of securing bus passengers is greater than the challenge of securing rail passengers.[90] Some transit systems have installed video cameras on their buses, but the number and operating characteristics of transit buses make them nearly impossible to secure. Because the volume of ridership and number of access points make it impractical to subject all rail passengers to the type of screening all airline passengers undergo, transit security measures tend to emphasize managing the

[85] See CRS Insight IN12476, *Drone Encounters Prompt Calls for Restrictions and Other Protections*, by Bart Elias.

[86] This section was prepared by Jennifer J. Marshall, CRS Analyst in Transportation Policy, with contributions from David Randall Peterman, former CRS Analyst in Transportation Policy.

[87] Amtrak is an intercity passenger rail service that operates over 21,300 route miles and has more than 500 stations.

[88] Federal Transit Administration, *2023 National Transit Summaries and Trends*, 2024, p. 11, https://www.transit.dot.gov/sites/fta.dot.gov/files/2024-10/2023%20National%20Transit%20Summaries%20and%20Trends_1.0.pdf.

[89] American Public Transportation Association (APTA), *2023 Public Transportation Fact Book*, March 2024, p. 6, https://www.apta.com/wp-content/uploads/APTA-2023-Public-Transportation-Fact-Book.pdf.

[90] APTA, *2023 Public Transportation Fact Book*, p. 6 and p. 15, Figure 13, "Revenue Vehicles Available for Maximum Service."

consequences of an attack. Nevertheless, steps have been taken to try to reduce the risk of an attack, including

- vulnerability assessments;
- emergency planning;
- emergency response training and drilling of transit personnel (ideally in coordination with police, fire, and emergency medical personnel);
- increasing the number of transit security personnel;
- installing video surveillance equipment in vehicles and stations; and
- conducting random inspections of bags, platforms, and trains.

In contrast with the aviation sector, where TSA provides security directly, security in surface transportation is provided primarily by the public and private transit and rail operators and local law enforcement agencies. TSA's main roles in surface transportation security are oversight, coordination, intelligence sharing, training, and assistance. It also provides some operational support through its Visible Intermodal Prevention and Response (VIPR) teams, which conduct operations with local law enforcement officials, including periodic patrols of transit and passenger rail systems to create "unpredictable visual deterrents."[91] Several presidential Administrations have sought to reduce the size of or eliminate the VIPR program;[92] prior Congresses have sought to increase the size of the program.[93]

Congressional efforts to promote transit and passenger rail security include providing grants to the service providers, requiring those providers considered to be high-risk targets (by DHS) to have their security plans approved by DHS, and requiring DHS to conduct security background checks and immigration status checks on all transit and railroad frontline employees.

According to TSA, its five primary objectives for reducing risk in transit and passenger rail are to

1. compose security plans that address critical infrastructure, cybersecurity, and operational practices to reduce terrorism threats;
2. provide training to security-sensitive employees;[94]
3. use exercises to identify opportunities to improve resilience;
4. increase timeliness of intelligence to industry stakeholders to enhance domain awareness; and
5. engage public and transit operators in the counterterrorism mission.[95]

[91] 6 U.S.C. §1112.

[92] DHS, Office of the Inspector General, *Federal Air Marshal Service Needs to Demonstrate How Ground-Based Assignments Contribute to TSA's Mission*, OIG-18-70, July 24, 2018.

[93] TSA, "A Review of the Fiscal Year 2025 Budget Request for the Transportation Security Administration," press release, May 15, 2024, https://www.tsa.gov/news/press/testimony/2024/05/15/review-fiscal-year-2025-budget-request-transportation-security; and DHS, (DHS), *Transportation Security Administration Budget Overview, Fiscal Year 2025 Congressional Justification*, p. 50.

[94] TSA, "Security Training for Surface Transportation Employees," 85 *Federal Register* 16456, March 23, 2020, https://www.federalregister.gov/documents/2021/05/04/2021-09394/security-training-for-surface-transportation-employees-extension-of-compliance-dates-correcting.

[95] TSA, *2023 Biennial National Strategy for National Security*, April 18, 2023, p. 66, https://www.dhs.gov/sites/default/files/2023-06/NSTS_Appendices_Final_4_18_23_508C.pdf.

Surface Transportation Security Inspectors Program

TSA's Surface Transportation Security Inspection Program was established in 2004 and conducts assessments of mass transit, passenger rail, highways, and motor carriers through the agency's voluntary Baseline Assessment for Security Enhancement (BASE) program. In compliance with TSA's "Security Training for Surface Transportation Employees" final rule of March 2020, surface inspectors are expected to perform security training program inspections of high-risk surface transportation owners and operators. Although the number of surface inspectors declined from 404 in FY2011 to 194 in FY2022 (because of achieved agency efficiencies, according to TSA), TSA indicated that current staffing levels should be sufficient to complete security training inspections required by the 2020 final rule.[96] In 2017, GAO reported that surface inspectors were consistently assigned to lower-risk surface transportation modes and non-surface transportation modes. Following the review of TSA's Surface Transportation Security Inspector Operations Plan, GAO recommended that TSA establish activity-level performance targets for the surface inspection program, which TSA began implementing in August 2021.[97]

Passenger Rail Security

TSA's incident reporting practices, development of process guidance, and stakeholder engagement practices regarding passenger rail security have been of interest to Congress. GAO reported in 2014 that TSA surface inspectors and rail agencies inconsistently reported rail security incidents because of the lack of agency guidance.[98] GAO also found that TSA did not have a systematic process for collecting and addressing feedback from surface transportation stakeholders regarding the effectiveness of the agency's information sharing effort.[99] In a 2015 hearing, GAO testified that TSA had put processes in place to address these issues.[100]

According to a 2020 GAO report, from 2009 through 2019, TSA participated in working groups with domestic stakeholders, such as the American Public Transit Association, to develop standards and best practices for passenger rail security.[101] In 2023, TSA partnered with Amtrak to perform security exercises in Maine and Connecticut through VIPR, sponsor canine training in Philadelphia, and support the Empire Line's NY SECURE exercises with TSA surface inspectors.[102] GAO also noted in the 2020 report that TSA's relationship with foreign stakeholders

[96] U.S. Congress, House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, *Lost in the Shuffle: Examining TSA's Management of Surface Transportation Security Inspectors*, 111th Cong., 2nd sess., July 28, 2010, H.Hrg. 66–028, p. 11; and GAO, *Surface Transportation: TSA Implementation of Security Training Requirement*, GAO-22-105315, April 2022, p. 18, https://www.gao.gov/assets/gao-22-105315.pdf.

[97] GAO, *Surface Transportation Security: TSA Has Taken Steps to Improve its Surface Inspector Program, but Lacks Performance Targets*, GAO-20-558, July 27, 2020, https://www.gao.gov/assets/gao-20-558.pdf.

[98] GAO, *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*, GAO-13-20, December 19, 2012.

[99] GAO, *Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts*, GAO-14-506, June 24, 2014.

[100] GAO, *Surface Transportation Security: TSA Has Taken Steps Designed to Develop Process for Sharing and Analyzing Information and to Improve Rail Security Incident Reporting*, GAO-15-205T. This GAO report was given in U.S. Congress, House Committee on Homeland Security, Subcommittees on Transportation Security and Counterterrorism & Intelligence, 114th Cong., 2nd sess., September 17, 2015.

[101] GAO, *Surface Transportation Security: TSA Has Taken Steps to Improve Its Surface Inspector Program*, GAO-20-558.

[102] Amtrak Police Department, *2023 Annual Report*, 2024, pp. 23, 34, https://police.amtrak.com/content/dam/projects/dotcom/english/public/documents/apd/apd-annual-report-2023.pdf.

in passenger rail could improve. In 2023, TSA, Amtrak, and Transport Canada partnered to conduct an inaugural international passenger railway security exercise as part of TSA's Surface Operations Exercise Information System Program.[103]

Transit Security Grant Program

DHS's Federal Emergency Management Agency (FEMA) provides grants for security improvements to public transit, passenger rail, and occasionally other surface transportation modes under the Transit Security Grant Program (TSGP; see **Table 1**).[104] The majority of the funding goes to public transit providers. According to GAO, 75% of grants for FY2015-FY2021 were awarded to public transit agencies for law enforcement activities and equipment.[105]

Continued oversight of the TSGP awarding process may be of interest to the 119th Congress. Congressional appropriators have expressed concern that significant amounts of previously appropriated funds under this program have not yet been awarded to recipients. In the 116th and 117th Congresses, stand-alone legislation was proposed to modify the period of performance of grant recipients and to extend the duration that grant funds are available to grant recipients.[106]

Congressional appropriators have also expressed concern that grants awarded under TSGP have not focused on areas of highest risk. GAO reported in 2023 that FEMA needed to improve transparency of the TSCP's grant decisions because higher-scoring applications were not always selected for awards in FY2015-FY2021, according to the selection criteria published in the notice of funding opportunity (NOFO). GAO provided four recommendations for improvement: (1) ensure that the NOFO accurately describes application scoring criteria, (2) ensure that grant award recommendations align with FEMA's public merit review process, (3) ensure that cyberthreats are incorporated into the risk model, (4) and document the underlying assumptions of the risk model. GAO said DHS had partially addressed the first three recommendations and fully addressed the last recommendation.[107]

Past Congresses have expressed concern about the relationship between the TSGP and other DHS programs, such as the State Homeland Security Program, Urban Areas Security Initiative, and Port Security Grant Program. In a 2012 report, GAO found potential for duplication among four DHS state and local security grant programs with similar goals, one of which was the TSGP. Congress has not supported consolidation of the programs.

[103] TSA, "TSA Conducts International Exercise Focusing on Threats to Cross Border Systems with Amtrak, Transport Canada," press release, December 15, 2023, https://www.tsa.gov/news/press/releases/2023/12/15/tsa-conducts-international-exercise-focusing-threats-cross-border.

[104] TSA uses information from the voluntary Baseline Assessment for Security Enhancement program and other sources to determine grant allocation priorities. See GAO, *Transit Security: FEMA Should Improve Transparency of Grant Decisions*, GAO-23-105956, July 2023, p. 25, https://www.gao.gov/assets/gao-23-105956.pdf.

[105] GAO, *Transit Security*, GAO-23-105956, p. 13.

[106] H.R. 396 (117th Congress); H.R. 1313 (116th Congress). Each bill was passed by the House but not by the Senate.

[107] GAO, *Transit Security*, GAO-23-105956.

Table 1. Congressional Funding for Transit Security Grants, FY2002-FY2024

Fiscal Year	Appropriation ($ millions of nominal dollars)	Appropriation ($ millions of 2024 dollars)
2002	63[a]	86
2003	65	88
2004	50	67
2005	108	131
2006	131	169
2007	251	321
2008	356	446
2009	498[b]	621
2010	253	312
2011	200	242
2012	88[c]	105
2013	84	100
2014	90	105
2015	87	102
2016	87	102
2017	88	102
2018	88	100
2019	88	99
2020	88	98
2021	84	92
2022	93	99
2023	93	96
2024	88	88

Sources: For FY2002, see Department of Defense FY2002 Appropriations Act (P.L. 107-117); for FY2003, see FY2003 Emergency Wartime Supplemental Appropriations Act (P.L. 108-11); for FY2004, see Department of Homeland Security FY2004 Appropriations Act (P.L. 108-90); for FY2005-FY2011, see U.S. Government Accountability Office, *Homeland Security: DHS Needs Better Project Information and Coordination Among Four Overlapping Grant Programs*, GAO-12-303, February 2012, Table 1; and for FY2012-FY2024, see FEMA, "Transit Security Grant Program," last updated August 23, 2024, https://www.fema.gov/grants/preparedness/transit-security#totals.

Notes: The Transit Security Grant Program was formally established in FY2005; in FY2003-FY2004, grants were made through the Urban Areas Security Initiative. Does not include funding provided for security grants for intercity passenger rail (Amtrak), intercity bus service, and commercial trucking. Nominal dollar amounts adjusted to constant 2024 dollars for fiscal years using the Total Non-defense column from Table 10.1: Gross Domestic Product and Deflators Used in the Historical Tables: 1940-2029, initially published in the Historical Tables volume of the *Budget of the U.S. Government, Fiscal Year 2025*, https://www.govinfo.gov/app/details/BUDGET-2025-TAB/context.

a. Appropriated to Washington Metropolitan Area Transit Authority and the Federal Transit Administration.

b. Includes $150 million provided in the American Recovery and Reinvestment Act (P.L. 111-5).

c. Congress did not specify an amount for transit security grants but provided a lump sum for state and local grant programs, leaving funding allocations to the discretion of DHS.

Freight Rail Security[108]

Freight trains generate roughly 29% of all freight ton-miles across all transportation modes in the United States, transported along a railway network over 130,000 miles long.[109] In contrast to publicly owned and managed airports and transit systems, freight rail infrastructure and operations are almost entirely the responsibility of private companies, with the bulk of tracks and traffic controlled by the six largest ("Class I") rail carriers.[110] The size of the railway network and the variety of cargoes carried by railroads make it difficult to secure.

As with other surface transportation modes, the importance of maintaining physical security of the freight rail network received attention from Congress in the aftermath of the 9/11 attacks and other international terrorist attacks on transit and rail systems. The rail industry has adopted numerous standards and programs intended to improve security. In 2002, railroads implemented an industry-wide Security Management Plan, and rail carriers participate in an annual American Railroad Industry Joint Security Exercise to evaluate and update the plan.[111] The industry, working with the Federal Railroad Administration, which is responsible for railroad safety enforcement and reporting, also created the Railway Alert Network to facilitate information sharing about security incidents and concerns.

Pursuant to provisions of Title XV, Subtitle B, of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), TSA issued its first Rail Transportation Security regulations in 2008.[112] The 2008 rule directed all railroad carriers to permit TSA inspections on request, appoint a rail security coordinator, and report significant security concerns. Other requirements were issued to cover trains transporting "rail security-sensitive" materials, including procedures to locate railcars carrying such materials on request and to maintain chain of custody and control agreements for sensitive shipments through a list of TSA-designated high-threat urban areas. Additional regulations issued in 2020 established guidelines for training programs required for security-critical employees.[113]

A separate rule published by the Pipeline and Hazardous Materials Safety Administration (PHMSA) in 2008 defined which hazardous materials qualified as "rail security-sensitive" and implemented other data collection and risk analysis requirements.[114] More stringent safety measures were placed on "high-hazard flammable trains" (HHFTs, those carrying large quantities of flammable liquids) by PHMSA in 2015 in response to several high-profile train derailments. The 2023 derailment (of a non-HHFT) and spill in East Palestine, OH, prompted some Members

[108] This section was prepared by Ben Goldman, CRS Analyst in Transportation Policy.

[109] Department of Transportation (DOT), Federal Railroad Administration, "Freight Rail Overview," https://railroads.dot.gov/rail-network-development/freight-rail-overview.

[110] The six Class I carriers are CSX Transportation, Norfolk Southern Railway (NS), Union Pacific Railroad (UP), BNSF Railway, Canadian National (CN), and Canadian Pacific Kansas City (CPKC). A *Class I rail carrier* is defined as one having a total operating revenue of $900 million or more in inflation-adjusted 2019 dollars; see Title 49, Part 1201, of the *Code of Federal Regulations*.

[111] Association of American Railroads, "Freight Rail Security," https://www.aar.org/issue/freight-rail-network-security/.

[112] TSA, "Rail Transportation Security," 73 *Federal Register* 72130, November 26, 2008.

[113] 49 C.F.R. Part 1580, Subpart B.

[114] DOT, Pipeline and Hazardous Materials Safety Administration (PHMSA), "Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments," 73 *Federal Register* 20752, April 16, 2008.

of Congress to consider applying those elevated safety measures to a larger number of trains so that more shipments of hazardous materials would be subject to rigorous risk analysis.[115]

Rail carriers maintain their own police forces to protect their employees, passengers, property, equipment, and cargo moving in interstate or foreign commerce, as well as personnel or cargo vital to national defense. Railroad police officers are state-commissioned, but federal law permits railroad police officers to enforce the law of any jurisdiction in which that rail carrier owns property.[116] During the supply chain crisis that followed the start of the COVID-19 pandemic, images of looted train cargo strewn alongside tracks and rail yards in Los Angeles circulated in the media, and some railroads have been victims of what appeared to be targeted thefts of high-value goods.[117] Theft from railroad cars moving interstate or international freight has been a federal crime since at least 1913.[118]

Port and Maritime Security[119]

In the aftermath of the 9/11 attacks, the U.S. Customs Service (Customs; now CBP) and the Coast Guard identified a need to *push the borders out* (i.e., begin screening vessels and cargo before they reach a U.S. port).[120] The bulk of U.S. overseas trade is carried by ships thus the economic repercussions of a maritime terrorist attack could be significant. While the previous screening methods that occurred in U.S. ports were considered sufficient to intercept some illicit cargo (e.g., smuggled drugs), they could be insufficient to disrupt a terrorist threat such as explosives or chemical, biological, nuclear, or radiological materials. Thus, Customs instituted the "24-hour rule," requiring importers to submit shipment information to Customs (now CPB) a day before the shipment was to arrive at the *overseas port* of loading rather than submitting this information within days of its arrival at a *U.S. port*. CBP analyzes this information and other intelligence to flag shipments it believes are higher risk or have an unknown risk. Under the Container Security Initiative, those riskier shipments are examined by imaging machines or possibly unloaded and inspected before being loaded on a vessel. (It is practically impossible to examine shipping containers once they are aboard a vessel or while the ship is at sea.)[121]

Similarly, the Coast Guard recognized the need to extend terrorist screening beyond U.S. ports. It requires ships to announce and report their intended arrival four days before entering a U.S. harbor.[122] The Coast Guard examines the vessel's particulars, its crew, and past history to evaluate the security risk. The Coast Guard pressed for establishing international standards for port security at the International Maritime Organization so that overseas ports sending cargo to the United States would abide by the same security regulations as U.S. ports. The Coast Guard also visits foreign ports to assess their security measures.

---

[115] See CRS Report R47911, *Freight Rail Safety Issues in the 119th Congress*, by Ben Goldman.

[116] 49 U.S.C. §28101(a).

[117] Ari Ashe, "US Rail Cargo Crime on the Rise as Thieves, Methods Gain Sophistication," *Journal of Commerce*, May 31, 2024.

[118] 18 U.S.C. §§659 and 2117; see also 37 Stat. 670 (Feb. 13, 1913).

[119] This section was prepared by John Frittelli, CRS Specialist in Transportation Policy.

[120] U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Securing the Supply Chain – Part I*, hearing, 112th Cong., 2nd sess., H.Hrg. 112-65, February 7, 2012.

[121] U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Balancing Maritime Security and Trade Facilitation: Protecting Our Ports, Increasing Commerce and Securing the Supply Chain – Part I*, hearing, 112th Cong., 2nd sess., H.Hrg. 112-65, February 7, 2012.

[122] 33 C.F.R. §160.212.

In addition to pushing the borders out, these agencies have instituted multiple layers of security that cover the four main elements of maritime transportation: ports, vessels, cargo, and workers. CBP's Customs Trade Partnership Against Terrorism (C-TPAT) program identifies a series of practices importers are to follow that are designed to cover a shipper's entire supply chain—from the overseas point of origin to final delivery in the United States. For instance, C-TPAT includes procedures and independent checks when loading a shipping container and applying the seal on its doors to prevent tampering while in route. In addition to container inspection equipment installed at overseas ports, CBP has installed radiation portal monitors at each truck exit gate in U.S. ports.

The Coast Guard requires vessel owners, port authorities, and their terminal operators to submit security plans that describe their access control measures, drills, and exercises to respond to a security incident and other measures to secure their facilities.[123] The Coast Guard recognizes that U.S. ports vary greatly in terms of their geographies and the types of cargo they handle. Port security plans allow the industry to develop specific plans to address the unique vulnerabilities of each port.

A goal of the Coast Guard is *maritime domain awareness*—knowledge of the varied legitimate vessel activity taking place in a harbor (cargo, fishing, recreational) so as to spot any abnormal or suspicious activity. One aspect of this is requiring many vessels to be equipped with automatic identification systems (transponders). The Coast Guard and TSA have also instituted a port worker background check for longshoremen, truck drivers, vessel crews, and others who need access to port terminals. A transportation worker identification credential (TWIC) card must be obtained from TSA and renewed every five years.[124]

Congress authorized much of the Coast Guard's role in maritime security in the Maritime Transportation Security Act of 2002 (MTSA; P.L. 107-295) and CBP's role in the Security and Accountability for Every Port Act of 2006 (P.L. 109-347). Congress modified these maritime security programs in Division J of the FAA Reauthorization Act of 2018 (P.L. 115-254).

Cyberattacks on container shipping lines have drawn attention to cyber vulnerabilities in the maritime industry.[125] In June 2017, a cyberattack on Maersk Line, the largest container carrier, prevented the carrier from taking bookings and required it to close its U.S. terminals for two to three days. Less severe attacks affected COSCO SHIPPING in July 2018 and Mediterranean Shipping Company in April 2020. A cyberattack on CMA CGM container line in September 2020 affected its ability to accept cargo bookings. In February 2022, a cyberattack essentially shut down a large freight forwarder for three weeks.[126]

In addition to ports and shipping companies that use computer networks to book and track cargo, developments in electronic navigation (e-navigation)—involving the replacement of paper charts with electronic charts (commonplace) or the replacement of channel marker buoys with virtual aids to navigation (in progress)—could create vulnerabilities to cyberattacks. P.L. 115-254 incorporated cybersecurity as a required element in MTSA security plans for terminal and vessel operators. A provision in the National Defense Authorization Act for FY2021 (NDAA FY2021; P.L. 116-283, §8244) requires the Coast Guard to report on its response capabilities to cyber incidents on U.S.-flag vessels. In January 2025, the Coast Guard issued a final rule on

[123] 33 C.F.R. §§101 et seq.

[124] 49 C.F.R. §1572.

[125] CRS In Focus IF10920, *Cyber Supply Chain Risk Management: An Introduction*, by Chris Jaikaran, provides an overview of federal efforts to address cybersecurity.

[126] Newstex Blogs, "Expeditors International: Back on Track After Cyberattack," June 15, 2022.

cybersecurity requirements for U.S.-flag vessels and U.S. ports.[127] This rule does not pertain to foreign-flag vessels calling at U.S. ports, which carry the overwhelming bulk of U.S. overseas trade.

Congress is evaluating the potential security risks of maritime equipment produced in the People's Republic of China (PRC or China) and used in U.S. ports. About 80% of ship-to-shore cranes that unload and load container ships in U.S. ports were manufactured in China, and there is concern that the software elements of these cranes could be used to collect cargo information or disrupt cargo handling operations.[128] There is also concern over LOGINK, a port logistics information portal provided by China and commonly used in ports around the world. The Biden Administration sought to begin domestic manufacturing of port cranes, and the NDAA FY2024 (P.L. 118-31, §825) forbid awarding federal grants to a port using LOGINK. Members of the House Homeland Security Committee have asked the Coast Guard how it screens the arriving ships of COSCO SHIPPING, a major Chinese container carrier, when it submits its notice of arrival information, noting that the Department of Defense has listed this carrier as a Chinese military company.[129] China builds the majority of oceangoing cargo ships; it manufactures nearly all of the containers used in the world fleet and 86% of the intermodal chassis (the wheeled frames for moving containers by truck).[130] China is also the United States' largest overseas trading partner, and its government-subsidized provision of maritime equipment and engineering know-how facilitates trade. The maritime sector is a prominent element of the United States' overall strategy in its relations with China.[131]

Pipeline Security[132]

Securing the nation's energy pipelines from intentional disruption has long been considered a priority for Congress and federal agencies.[133] TSA's *2023 Biennial National Strategy for Transportation Security* identified both physical and cyber risks for pipelines.

> The national pipeline system and associated facilities are vulnerable ... largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline

[127] DHS, Coast Guard, "Final Rule: Cybersecurity in the Marine Transportation System," 90 *Federal Register* 6298, January 17, 2025, https://www.govinfo.gov/content/pkg/FR-2025-01-17/pdf/2025-00708.pdf.

[128] DHS, Coast Guard, "Issuance of Maritime Security (MARSEC) Directive 105-5; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies," 89 *Federal Register* 91413, November 19, 2024; and DHS, *U.S. Maritime Trade and Port Cybersecurity*, 2023, https://www.dhs.gov/sites/default/files/2024-09/2024aepphasellusmaritimetradeandportcybersecurity.pdf.

[129] Letter to The Honorable Admiral Kevin E. Lunday, acting commandant, Coast Guard, from Rep. Mark Green et al., January 22, 2025, https://homeland.house.gov/wp-content/uploads/2025/01/2025.01.22-Letter-to-USCG-re-COSCO-Shipping-Threats.pdf.

[130] Office of the U.S. Trade Representative, Section 301 Investigation, *Report on China's Targeting of the Maritime, Logistics, and Shipbuilding Sectors for Dominance*, January 16, 2025; https://ustr.gov/sites/default/files/enforcement/301Investigations/USTRReportChinaTargetingMaritime.pdf.

[131] CRS In Focus IF10119, *China Primer: U.S.-China Relations*, by Susan V. Lawrence and Karen M. Sutter.

[132] This section was prepared by Paul Parfomak, CRS Specialist in Energy Policy.

[133] For example, see U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Pipeline Cybersecurity: Protecting Critical Infrastructure*, hearing, 117th Cong., 1st sess., July 27, 2021; and U.S. Congress, House Committee on Homeland Security, Subcommittee on Management, Investigations, and Oversight, *Unclogging Pipeline Security: Are the Lines of Responsibility Clear?*, field hearing, 111th Cong., 2nd sess., H.Hrg. 111-62, April 19, 2010.

networks spanning urban and outlying areas. Pipeline systems may also be vulnerable to a cyber-attack due to their reliance on operational technology systems.[134]

After the 9/11 attacks, federal attention to pipeline security focused on physical threats from transnational terrorist groups, such as Al Qaeda. Since that time, pipeline threats have broadened to include both physical and cyberthreats from domestic extremists, transnational criminal groups, and nation-states.[135] The May 2021 ransomware attack on the Colonial Pipeline Company, which disrupted supplies of gasoline throughout the East Coast for several days, demonstrated the heightened vulnerability of pipelines to cyberattacks.[136] Subsequent events, such as the 2022 bombing of the Nord Stream natural gas pipelines in Europe and a 2023 plot to attack the Baltimore electricity grid, suggest that pipeline physical security continues to be a concern.[137]

TSA's Pipeline Security Program

Pipelines are part of the surface transportation critical infrastructure sector, for which TSA is the sector risk management agency and administers the federal program for pipeline security.[138] ATSA authorizes the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). In carrying out its mission, TSA cooperates with DOT's PHMSA, which also has certain pipeline security authorities, under the terms of a 2020 memorandum of understanding delineating their respective roles.[139]

Prior to the Colonial Pipeline cyberattack, TSA relied on industry's voluntary compliance with the agency's guidelines for pipeline physical security.[140] In 2003, TSA initiated its ongoing pipeline Corporate Security Review Program. Through this program, the agency conducts voluntary visits with pipeline operators "to assess the current security practices in the pipeline industry, with a focus on the physical and cyber security of pipelines."[141] The agency's reliance on voluntary compliance with recommended security standards has been questioned by some

[134] DHS, *2023 Biennial National Strategy for Transportation Security Appendices: Appendix C: Surface Security Plan*, April 18, 2023, p. 88, https://www.dhs.gov/sites/default/files/2023-06/NSTS_Appendices_Final_4_18_23_508C.pdf.

[135] TSA, *Biennial National Strategy for Transportation Security, Appendix C: Surface Security Plan*, pp. 88-89.

[136] Colonial Pipeline, "Media Statement Update: Colonial Pipeline System Disruption," press release, May 17, 2021, https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

[137] Adam Entous et al., "Intelligence Suggests Pro-Ukrainian Group Sabotaged Pipelines, U.S. Officials Say," *New York Times*, March 7, 2023; U.S. Attorney's Office, District of Maryland, "White Supremacist Leader Found Guilty of Conspiring to Destroy Regional Power Grid," press release, February 3, 2025, https://www.justice.gov/usao-md/pr/white-supremacist-leader-found-guilty-conspiring-destroy-regional-power-grid; and Letter to The Honorable Christopher Wray, Director, Federal Bureau of Investigation, from Rep. James Comer, Chairman, House Committee on Oversight and Accountability et al, April 15, 2024, https://oversight.house.gov/wp-content/uploads/2024/04/Briefing-Request-to-FBI-re-Ecoterrorism-041524.pdf.

[138] TSA, "Surface Transportation Resources," https://www.tsa.gov/for-industry/resources.

[139] TSA and PHMSA, Transportation Security Administration and Pipeline and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety, memorandum of understanding, February 26, 2020, https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/regulatory-compliance/phmsa-guidance/73466/phmsa-tsa-mou-annexexecuted.pdf.

[140] TSA, *Pipeline Security Guidelines*, March 2018 (with change 1 [April 2021]), https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

[141] TSA, "Intent to Request an Extension from OMB of One Current Public Collection of Information: Pipeline Corporate Security Review Program," 87 *Federal Register* 190, October 3, 2022, p. 59817.

stakeholders.[142] In 2021, following the Colonial Pipeline incident, TSA announced its first mandatory security directive applicable to owners and operators of critical pipeline facilities (as identified by TSA).[143] The directive required that companies designate and use a cybersecurity coordinator, conduct a cybersecurity vulnerability assessment, identify gaps, identify remediation measures, and establish a timeline to implement those measures. Companies were required to report this information to TSA and the Cybersecurity and Infrastructure Security Agency (CISA) within 30 days.[144]

On July 20, 2021, TSA announced a second security directive, requiring critical pipeline companies "to implement specific mitigation measures to protect against ransomware attacks and other known threats to information technology (IT) and operational technology (OT) systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review."[145] The security directives were to be effective for one year from the date of issuance, with the possibility of extension. The agency has since updated and reissued both directives, most recently with effective dates of May 29, 2024, and July 27, 2024, respectively.[146] As with the 2021 directives, the revised versions are effective for one year.

After the initial issuance of TSA's directives, some in industry were critical of TSA for issuing such directives under emergency authority rather than promulgating cybersecurity regulations through a traditional rulemaking process that would afford industry with opportunities to provide input.[147] The agency subsequently initiated a rulemaking process "seeking input regarding ways to strengthen cybersecurity and resiliency in the pipeline and rail" sectors.[148] On November 7, 2024, TSA published in the *Federal Register* a notice seeking comment on a proposed rule which, among other things, would "impose cyber risk management (CRM) requirements on certain pipeline and rail owner/operators" and require them "to have a Physical Security Coordinator and report significant physical security concerns."[149] The comment period was set at 90 days, through February 5, 2025. TSA has not initiated proceedings to establish mandatory requirements for pipeline physical security. Some pipeline companies have publicly reported physical security investments, but such measures remain voluntary.[150]

[142] Neil Chatterjee and Richard Glick, "Cybersecurity Threats to U.S. Gas Pipelines Call for Stricter Oversight," *Axios*, June 11, 2018, https://www.axios.com/2018/06/11/cybersecurity-threats-to-us-gas-pipelines-call-for-stricter-oversight.

[143] TSA Security Directive Pipeline-2021-01, *Enhancing Pipeline Cybersecurity*, May 27, 2021.

[144] TSA Security Directive Pipeline-2021-01, *Enhancing Pipeline Cybersecurity*, May 27, 2021.

[145] DHS, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," July 20, 2021, https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators. TSA's announcement did not provide specific details about security measures because they were considered sensitive security information (SSI).

[146] TSA Security Directive Pipeline-2021-01D, *Enhancing Pipeline Cybersecurity*, May 29, 2024, https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01d.pdf; and TSA Security Directive Pipeline-2021-02E, *Memorandum*, July 26, 2024, https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02e-and-memo-508c.pdf. The revised second directive is no longer considered SSI, although cybersecurity information submitted to TSA by operators remains confidential.

[147] Leticia Gonzales, "SA Adds More Stringent Cybersecurity Requirements for U.S. Natural Gas, Oil Pipelines," *Natural Gas Intelligence*, July 23, 2021.

[148] TSA, "Enhancing Surface Cyber Risk Management," 87 *Federal Register* 73527-73538, November 30, 2022.

[149] TSA, "Enhancing Surface Cyber Risk Management," 88 *Federal Register* 88488-88592, November 7, 2024.

[150] For example, see Northern Natural Gas, "Physical Security Enhancements Support Reliability," *Northern Notes*, April 2024, p. 4, https://www.northernnaturalgas.com/Document%20Postings/Northern%20Notes_April%202024.pdf.

Transportation Cybersecurity[151]

The transportation sector, as with all critical infrastructure sectors, faces cybersecurity risks. Several federal agencies are engaged in cybersecurity activities in the transportation sector, and TSA has taken a more active posture on cybersecurity regulations since 2021. Congress has expressed interest in TSA's management of cybersecurity, particularly as TSA shifts its approach from sub-sector specific (e.g., aviation or rail) to sector-wide cybersecurity, which could affect a broader set of companies.

Cyber Risks

During the 117th and 118th Congresses, numerous high-profile cybersecurity events affected the transportation sector, including the following selected events:

- In July 2024, a faulty update to widely used cybersecurity software disrupted airline computer systems, which led to thousands of flight cancellations, extensive delays, and long waits at airports.[152]
- In January 2023, hackers stole and leaked sensitive files from a public transit system.[153]
- In September 2022, a congressional commission highlighted risks related to a logistics management platform used in maritime transportation and shipping, as the platform could be used by the PRC to steal data or disrupt operations.[154]
- In May 2021, Colonial Pipeline halted operations to respond and recover from a ransomware attack.[155]

Several of these high-profile events reflect the ability and willingness of adversaries to target the transportation sector. Adversaries may seek to compromise the sector for its economic role in moving goods and services and for its national security importance. Rear Admiral Mark Montgomery (Ret.), former executive director of the Cyberspace Solarium Commission, testified before the House Committee on Homeland Security on the importance of the transportation sector:

> The purpose of the CCP's [Chinese Communist Party's] cyberattacks is not just to sow chaos or intimidate civilians. Chinese leaders understand that America will struggle to rapidly mobilize military forces if the rail, aviation, and port systems that move military equipment, personnel, and supplies to the battlefield are degraded or inoperable.[156]

[151] This section was prepared by Chris Jaikaran, CRS Specialist in Cybersecurity Policy.

[152] For more information, see CRS Insight IN12392, *The July 19th Global IT Outages*, by Chris Jaikaran.

[153] Kevin Collier, "Hackers Leak Sensitive Files After Attack on San Francisco Transit Police," *NBC News*, January 10, 2023, https://www.nbcnews.com/tech/security/hackers-leak-sensitive-files-attack-san-francisco-transit-police-rcna65071.

[154] U.S.-China Economic and Security Review Commission, *LOGINK: Risks from China's Promotion of a Global Logistics Management Platform*, September 10, 2022, https://www.uscc.gov/sites/default/files/2022-09/LOGINK-Risks_from_Chinas_Promotion_of_a_Global_Logistics_Management_Platform.pdf.

[155] For more information, see CRS Insight IN11667, *Colonial Pipeline: The DarkSide Strikes*, by Paul W. Parfomak and Chris Jaikaran.

[156] Testimony of Rear Admiral Mark Montgomery (Ret.) in U.S. Congress, House Committee on Homeland Security, *Unconstrained Actors: Assessing Global Cyber Threats to the Homeland*, hearing, 119th Cong., 1st sess., January 22, 2025, https://homeland.house.gov/hearing/unconstrained-actors-assessing-global-cyber-threats-to-the-homeland.

Relevant Agencies

Transportation is one of the 16 critical infrastructure sectors established in U.S. policy.[157] A sector's sector risk management agency (or agencies) is responsible for working with industry and CISA to promote sector-wide security—including cybersecurity. The transportation sector is divided into seven subsectors or modes: aviation, highway and motor carrier, maritime, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping. DHS and DOT share responsibility for the sector. DHS manages transportation sector security through TSA, which has regulatory authority over transportation sector security broadly, and the Coast Guard, which has regulatory authority over maritime safety and security. DOT manages the sector through its Office of Intelligence, Security, and Emergency Response. In addition, DOT has regulatory authority over pipelines through PHMSA and aviation through FAA.[158]

TSA Approaches to Cybersecurity

TSA's initial approach to transportation sector cybersecurity through voluntary collaboration with industry was controversial. As early as 2008, a DOT Inspector General report stated that "TSA's current security guidance is not mandatory and remains unenforceable unless a regulation is issued to require industry compliance."[159]

In November 2018, TSA released a cybersecurity roadmap establishing a broad framework for how it engages with transportation industry and government stakeholders to address cybersecurity risks.[160] The *Cybersecurity Roadmap* identified strategic priorities for cybersecurity, which included

- assessing and prioritizing evolving cyber risks to transportation sector systems;
- reducing vulnerabilities through protective and preventive measures;
- mitigating consequences through coordinated response efforts;
- strengthening security and resilience of information and communications technology systems across the transportation sector; and
- promoting collaborative efforts to improve management of cybersecurity activities.[161]

Following the Colonial Pipeline attack in 2021, TSA moved toward mandatory standards. The agency issued security directives requiring critical pipeline operators to have a cybersecurity

[157] White House, "Delegation of Authority Under Section 614(a)(1) and Section 506(a)(1) of the Foreign Assistance Act of 1961," presidential memorandum of September 21, 2023, 88 *Federal Register* 195, October 11, 2023.

[158] In October 2021, the PHMSA acting administrator stated that the agency's security role "includes coordination efforts with the Transportation Security Administration and other federal agencies to ensure there is a collaborative and efficient approach to monitoring, inspecting, and promulgating regulations related to cybersecurity in the pipeline industry" (see PHMSA, "Remarks of PHMSA Acting Administrator Tristan Brown Before the AOPL-API Fall Meeting," October 14, 2021, https://www.phmsa.dot.gov/news/remarks-phmsa-acting-administrator-tristan-brown-aopl-api-fall-meeting).

[159] DOT Office of Inspector General, "Actions Needed to Enhance Pipeline Security," AV-2008-053, May 21, 2008, p. 6, https://www.oig.dot.gov/sites/default/files/Pipeline_Security_Report_reissued_AV-2008-53.pdf. Provisions in the Pipeline Inspection, Protection, Enforcement, and Safety Act of 2006 (P.L. 109-468) required the Inspector General to "address the adequacy of security standards for gas and oil pipelines" (§23(b)(4)).

[160] TSA, *TSA Cybersecurity Roadmap 2018*, November 2018, https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf.

[161] TSA, *TSA Cybersecurity Roadmap 2018.*

coordinator, report incidents, assess cyber vulnerabilities, and implement prescriptive measures and practices to defend against cyber threats.

Since the directives were issued in 2021, TSA has issued more than 20 security directives related to cybersecurity for the pipeline and rail sectors.[162] These directives require a variety of actions, including assigning responsibilities to specific company employees, planning, vulnerability assessments, and incident reporting.

TSA's authority to issue security-related directives is derived from its authority to regulate the transportation industry for security purposes.[163] TSA's authority allows the agency to issue binding directives quickly in an emergency. The authority does not absolve TSA from following the Administrative Procedure Act (APA) for notice and deliberation in rulemaking.[164]

In response to requests from industry to engage in the APA rulemaking processes, TSA issued an advance notice of proposed rulemaking (ANPRM) on "Enhancing Surface Cyber Risk Management" in 2022.[165] This notice provided a public record of how TSA considers cyber risk management issues, which standards it intends to follow, which sectors it seeks to regulate (i.e., pipelines and rail), and how the public can provide input under the rulemaking process.

Following the 2022 APNRM, TSA released a notice of proposed rulemaking (NPRM) related to pipeline and rail cyber risk management on November 7, 2024.[166] The proposed rule would mandate that rail and pipeline companies (1) have a TSA-approved cyber risk management program that would include evaluations, plans, and prescribed security outcomes; (2) require cyber incident reporting to CISA; and (3) account for physical security concerns.[167] The comment period for the NPRM closed on February 5, 2025.

Author Information

Bart Elias, Coordinator
Specialist in Aviation Policy

Chris Jaikaran
Specialist in Cybersecurity Policy

John Frittelli
Specialist in Transportation Policy

Jennifer J. Marshall
Analyst in Transportation Policy

Ben Goldman
Analyst in Transportation Policy

Paul W. Parfomak
Specialist in Energy Policy

[162] TSA, "Security Directives and Emergency Amendments," https://www.tsa.gov/sd-and-ea.

[163] 49 U.S.C. §114(l).

[164] 5 U.S.C. §553. The Administrative Procedure Act is at 5 U.S.C. §§551 et seq.

[165] TSA, "Enhancing Surface Cyber Risk Management," 87 *Federal Register* 73527-73538, November 30, 2022.

[166] TSA, "Enhancing Surface Cyber Risk Management," 89 *Federal Register* 88488-88592, November 7, 2024.

[167] TSA, "TSA Announces Proposed Rule That Would Require the Establishment of Pipeline and Railroad Cyber Risk Management Programs," press release, November 6, 2024, https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and.

Disclaimer