Congressional Research Service
Informing the legislative debate since 1914

Transportation Security: Background and Issues for the 117th Congress

February 9, 2021

Congressional Research Service
https://crsreports.congress.gov
R46678

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46678

February 9, 2021

Bart Elias
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

David Randall Peterman
Analyst in Transportation Policy

Transportation Security: Background and Issues for the 117th Congress

The nation's air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them vulnerable to terrorist attack. While hardening the transportation sector is difficult, measures can be taken to deter terrorists. The enduring challenge facing Congress is how best to implement and finance a system of deterrence, protection, and response that effectively reduces the possibility and consequences of terrorist attacks without unduly 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 moved quickly to pass 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, their baggage, and air cargo. Despite attention to aviation and transportation security over the past two decades, a number of challenges remain, including

- developing and deploying effective biometric capabilities to verify the identities of transportation workers and travelers;
- developing effective risk-based approaches to vetting and screening transportation workers accessing 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 effectively deter and respond to criminal and terrorist acts targeting public areas of transportation facilities.

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. Oversight of TSA actions to implement these mandates may be an area of particular interest in the 117th Congress. Particular topics may include

- the evolution of screening technologies and assessments of emerging screening technology solutions;
- TSA enforcement of a federal mask mandate during the Coronavirus Disease 2019 (COVID-19) pandemic;
- proposals to expand the use of canine teams for transportation security;
- the use of terrorist watchlists to deny boarding and identify individuals for enhanced security screening, and the possible inclusion of U.S. citizens involved in violent anti-government activities on those lists;
- the expansion of the PreCheck program to expedite screening of known travelers;
- the use of biometrics and associated data security and privacy concerns;
- implementing effective approaches, regulations, and international agreements to conduct risk-based screening of air cargo shipments worldwide;
- protecting public areas of airports; and
- developing effective countermeasures to protect critical infrastructure, including airports and aircraft, from attacks and interference from drones and possible terrorist attacks using shoulder fired missiles.

Bombings of passenger trains in Europe and Asia in the past few years illustrate the vulnerability of passenger rail systems to terrorist attacks. Passenger rail systems—primarily subway systems—in the United States carry about five times as many passengers each day as do airlines, over many thousands of miles of track, serving stations that are designed primarily for easy access. Transit security issues of recent interest to Congress include the quality of TSA's surface transportation inspector program. The bulk of U.S. overseas trade is carried by ships, and thus the economic consequences of a maritime terrorist attack could be significant. Customs and Border Protection (CBP) and the Coast Guard have implemented security screening procedures that effectively "push the borders out"—that is, they begin screening vessels and cargo before they reach a U.S. port. Two aspects of maritime security that have drawn attention recently are cybersecurity and the use of drones for coastal surveillance.

Contents

Tables

Contacts

Introduction

The nation's air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them vulnerable to attack. The difficulty and cost of protecting the transportation sector from attack raises a core question for policymakers: how much effort and resources to put toward protecting potential targets versus pursuing and fighting terrorists. While hardening the transportation sector against terrorist attack is difficult, measures can be taken to deter terrorists. The focus of debate is how to implement and finance a system of deterrence, protection, and response that effectively reduces the possibility and consequences of terrorist attacks without unduly interfering with travel, commerce, and civil liberties.

For all modes of transportation, one can identify four principal policy objectives that would 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 the transportation workers who operate and service the vehicles, assist the passengers, or handle the cargo; (3) ensuring the trustworthiness of the private companies that operate in the system, such as the carriers, shippers, agents, and brokers; and (4) establishing a perimeter of security around transportation facilities and vehicles in operation.

The first three policy objectives are concerned with preventing attacks from within a transportation system, such as the attacks that occurred on September 11, 2001. The concern is that attackers could once again disguise themselves as legitimate passengers (or shippers or workers) to launch an attack.

The fourth policy objective is concerned with preventing an attack 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 taking off or landing, as was attempted in November 2002 against an Israeli charter jet in Mombasa, Kenya.

Achieving all four of these objectives is difficult at best, and in some modes, is practically impossible. Where limited options exist for preventing an attack, policymakers are left with evaluating options for minimizing the consequences of an attack, without imposing unduly burdensome requirements.

Aviation Security[1]

Following the 9/11 terrorist attacks, Congress created the Transportation Security Administration (TSA) within the U.S. Department of Transportation, giving it control over all airline passenger and baggage screening functions and deployment of armed air marshals on commercial passenger flights. In 2003, TSA was transferred to the newly formed Department of Homeland Security (DHS).[2]

In addition to its primary role to protect transportation facilities and assets from terrorist and criminal threats, TSA plays a central role in enforcing a federal mask mandate implemented in response to the Coronavirus Disease 2019 (COVID-19) pandemic. In accordance with Executive Order 13998 on Promoting COVID-19 Safety in Domestic and International Travel and CDC orders and guidelines, TSA is expected to enforce requirements that individuals wear masks at

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

[2] See P.L. 107-296.

airport screening checkpoints and throughout commercial and public transportation systems including at stations, ports, and other transportation hubs.[3]

The federal role in airport screening remains controversial. While airports are allowed to opt out of federal screening, alternative private screening under TSA contracts has been limited to 22 airports out of approximately 450 commercial passenger airports where passenger screening is required.[4] Congress has sought to ensure that optional private screening remains available for those airports that want to pursue this option. The TSA Modernization Act, incorporated into the FAA Reauthorization Act of 2018 (P.L. 115-254), 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 program to allow individual airport terminals, instead of entire airports, to switch over to screening by private contractors. Proposals seeking more extensive reforms of passenger screening have not been extensively debated. Rather, aviation security legislation has largely focused on specific mandates to comprehensively screen for explosives and carry out background checks and threat assessments.

Despite the attention to aviation security for more than a decade, a number of challenges remain, including

- effectively screening passengers, baggage, and cargo for explosives threats;
- developing effective risk-based methods for screening passengers and others with access to aircraft and sensitive areas;
- incorporating biometrics into the passenger screening process to verify identities;
- exploiting available intelligence information and watchlists to identify individuals who pose potential threats to civil aviation;
- implementing effective systems, regulations, and international agreements to assess risk and conduct risk-based screening of air cargo shipments worldwide;
- effectively deterring and responding to security threats in public areas of airports and at screening checkpoints;
- developing effective strategies for addressing aircraft vulnerabilities to shoulder-fired missiles and other external threats like rocket-propelled grenades; and
- addressing the potential security implications of unmanned aircraft operations in domestic airspace and developing effective countermeasures to protect critical infrastructure, including airports and aircraft, from attacks using drones.

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. Immediately following the 9/11 attacks, the Aviation and Transportation Security Act (ATSA; P.L.

[3] Transportation Security Administration, "TSA to implement Executive Order regarding face masks at airport security checkpoints and throughout the transportation network," National Press Release, January 31, 2021, https://www.tsa.gov/news/press/releases/2021/01/31/tsa-implement-executive-order-regarding-face-masks-airport-security#:~:text=WASHINGTON%20%E2%80%93%20The%20Transportation%20Security%20Administration,well%20as%20while%20on%20passenger.

[4] Transportation Security Administration, *Screening Partnership Program*, https://www.tsa.gov/for-industry/screening-partnerships.

107-71) 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. Rather, TSA satisfies this mandate through the Certified Cargo Screening Program. Under the program, manufacturers, warehouses, distributors, freight forwarders, and shippers carry out screening inspections using TSA-approved technologies and procedures both at airports and at 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 continue to pilot test the Air Cargo Advance Screening (ACAS) system, initiated 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 review and improve the Known Shipper Program and Certified Cargo Screening Program 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.

Separately, new international security requirements stipulate that by June 30, 2021, all inbound and outbound international air cargo, whether it be carried on passenger or all-cargo aircraft, must be screened before being placed onboard an aircraft unless it is received from a TSA-approved shipper that applies acceptable security controls and/or screening protocols.[5]

Given the focus on the threats to aviation posed by explosives, a significant focus of TSA acquisition efforts has been on 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. P.L. 115-254 required TSA to update the technology investment plan annually to accompany 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.

[5] Transportation Security Administration, "Air Cargo Security Options To Mitigate Costs of Compliance With International Security Requirements," 85 *Federal Register* 20234-20238, April 10, 2020.

A major thrust 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,[6] 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 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.[7] 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. Most recently, TSA has begun to field CT-based Explosive Detection Systems, similar to those used to screen checked baggage at passenger screening checkpoints to scan carry-on items. TSA is deploying about 300 advanced technology screening systems with CT capability to the busiest airports, and plans to begin rolling out next-generation CT-based Checkpoint Property Screening Systems (CPSS) between 2020 and 2025. TSA's long-term goal is to deploy CPSS with "auto-detect" capabilities that would only project an image to human screeners when an alert occurs which could improve checkpoint screening efficiency and reduce staffing requirements.[8]

The use of AIT raised a number of policy questions. Privacy advocates objected to the intrusiveness of AIT, particularly when used for primary screening.[9] To allay privacy concerns, TSA 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 automated targeting recognition (ATR) software. Another concern raised about AIT centered on the potential medical risks posed by backscatter X-ray systems, but those systems are no longer in use for airport screening, and current millimeter wave systems emit nonionizing millimeter waves generally not considered harmful.[10] 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.[11] Physical pat downs to resolve AIT alarms remain controversial because of their intrusiveness as well as questions about the effectiveness of pat down techniques to detect well concealed threat items.

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

[7] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York, NY: W. W. Norton & Co., 2004).

[8] Transportation Security Administration, *Capital Investment Plan, FY2021-FY2025,* June 30, 2020, https://www.dhs.gov/sites/default/files/publications/tsa_-_capital_investment_plan_fy_2021-fy_2025.pdf.

[9] See, e.g., American Civil Liberties Union. ACLU Backgrounder on Body Scanners and "Virtual Strip Searches," New York, NY, January 8, 2010.

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

[11] Statement of John Roth, Inspector General, Department of Homeland Security, Before the Committee on Oversight and Government Reform, U.S. House of Representatives, Concerning TSA: Security Gaps, November 3, 2015.

Even prior to the revelations of weaknesses in passenger checkpoint screening technologies and procedures, the use of AIT was controversial. Past legislative proposals specifically sought to prohibit the use of whole body imaging for primary screening (see, for example, H.R. 2200, 111th Congress). Primary screening using AIT is now commonplace at larger airports, but checkpoints at many smaller airports have not been furnished with AIT equipment and other advanced checkpoint detection technologies. This raises questions about TSA's long-range plans to expand AIT to ensure more uniform approaches to explosives screening across all categories of airports.

Through FY2020, TSA has deployed about 950 AIT units and has updated hardware and software of fielded units to improve threat detection and increase service life. It has not planned for procurements beyond this level, although many smaller airports are not equipped with this capability.[12] TSA plans to manage this risk to a large extent through risk-based passenger screening measures, primarily through increased use of voluntary passenger background checks under the PreCheck trusted traveler program. However, this program's incentive of expedited screening is offered at fewer than half of all commercial passenger airports in the United States.

The FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) directed TSA to initiate a demonstration program at three to six large airports to examine passenger checkpoint reconfigurations that increase efficiencies and reduce vulnerabilities, and a separate demonstration program at three airports to develop and test next-generation screening system prototypes designed to expedite passenger handling. P.L. 115-254 instructed TSA to continue operation of its systems integration facility at Washington Reagan National Airport for testing and evaluating advanced transportation security screening technologies, and to ensure timely assessments of new screening technologies. It also directed TSA to encourage private firms to develop and commercialize new transportation security technologies and to establish an innovation task force to accelerate the development of innovative technologies. While TSA has set up the innovation task force and is seeking to foster demonstrations of novel security technologies,[13] an October 2020 Government Accountability Office (GAO) performance audit found that TSA had not yet established effective metrics and mechanisms to integrate and evaluate private industry testing of candidate systems.[14]

The act also 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 by another DHS entity. The laboratory was originally transferred to TSA from the Federal Aviation Administration (FAA), but has been in the hands of the DHS Science and Technology (S&T) Directorate for more than a decade. The S&T Directorate continues to operate the TSL while TSA operates its Systems Integration Facility in Washington, DC, which is responsible for more advanced qualification testing of technologies and conducts operational testing of promising 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, but GAO found in 2020 that TSA lacked specific metrics

[12] Department of Homeland Security, *Transportation Security Administration Fiscal Year 2021 Congressional Justification, Operations and Support*, https://www.dhs.gov/sites/default/files/publications/transportation_security_administration.pdf.

[13] For more on the Innovation Task Force, see https://www.tsa.gov/itf.

[14] U.S. Government Accountability Office, *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.

for evaluating third-party testing protocols, something it considered critical to assessing whether the third-party testing concept contributes to supplier diversity and innovation objectives.[15]

Risk-Based Passenger Screening

TSA has initiated a number of risk-based screening initiatives to focus its resources and apply directed measures based on intelligence-driven assessments of security risk. These include PreCheck; modified screening procedures for children 12 and under; and a program for expedited screening of known flight crew and cabin crew members. Programs have also been developed for modified screening of elderly passengers similar to those procedures put in place for children.

PreCheck is modeled on CBP programs such as Global Entry, SENTRI, and NEXUS. Under the program, participants vetted through a background check process are processed through expedited screening lanes where they can keep shoes on and keep liquids and laptops inside carry-on bags. As of December 2020, PreCheck expedited screening lanes were available at more than 200 airports. The cost of background checks under the PreCheck program is recovered through application fees of $85 per passenger for a five-year membership. TSA's goal is to process 50% of passengers through PreCheck expedited screening lanes, thus reducing the need for standard security screening lanes, but it has struggled to increase program membership. More than 9 million travelers had enrolled in PreCheck as of August 2019.[16] Roughly an additional 9 million are considered eligible to use PreCheck expedited screening lanes based on enrollment in Global Entry, or in some cases SENTRI, or NEXUS.[17]

One concern raised over the PreCheck program is the lack of biometric authentication to verify participants at screening checkpoints. A predecessor test program, the Registered Traveler program, which used private vendors to issue and scan participants' biometric credentials, 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. Participants in Clear, which is separate from PreCheck and not operated or funded by TSA, use an express lane to verify identity using a fingerprint or iris scan rather than interacting with a TSA document checker.[18]

Previously, the extensive use of a program called "managed inclusion" to route selected travelers not enrolled in PreCheck through designated PreCheck expedited screening lanes also raised objections. GAO found that TSA had not fully tested its managed inclusion practices, and recommended that TSA take steps to ensure and document that testing of the program adheres to established evaluation design practices.[19]

TSA phased out the managed inclusion program in fall 2015. Since September 2015, TSA behavior detection officers and explosives trace detection personnel no longer direct passengers

[15] Ibid.

[16] Department of Homeland Security, *Transportation Security Administration Fiscal Year 2021 Congressional Justification, Operations and Support,* https://www.dhs.gov/sites/default/files/publications/transportation_security_administration.pdf.

[17] Department of Homeland Security, *Customs and Border Protection Fiscal Year 2021 Congressional Justification, Global Entry Fee*, https://www.dhs.gov/sites/default/files/publications/u.s._customs_and_border_protection.pdf; Department of Homeland Security, *Trusted Traveler Programs,* https://ttp.dhs.gov/.

[18] 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.

[19] U.S. Government Accountability Office, *Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments*, GAO-15-150, December 2014.

not enrolled in PreCheck to expedited screening lanes, but pre-assessments using canine teams have continued at some major airports. Questions remain regarding whether PreCheck is fully effective in directing security resources to unknown or elevated-risk travelers. Nonetheless, it has improved screening efficiency. In 2016, TSA estimated annual savings in direct screener workforce costs totaling $110 million as a result of PreCheck and other risk-based initiatives.[20] A study the following year 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 to 20 million.[21] Oversight of TSA efforts to expand PreCheck may be a specific topic of interest during the 117th Congress.

Congress in 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. The most recent publicly available data suggest that TSA was having difficulty meeting this target even before the COVID-19 pandemic reduced air travel.

The act required TSA to ensure that PreCheck expedited screening lanes are open and available to program participants during peak and high-volume travel times and take steps to provide expedited screening at standard screening lanes when PreCheck lanes are not available. 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.

P.L. 115-254 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 Biometrics Roadmap,[22] TSA also plans to integrate biometrics technology for identity verification of PreCheck travelers, and seeks to eventually expand the voluntary use of biometrics to all domestic air travelers. Plans for increased use of biometrics raise privacy and data-protection concerns that may be of particular interest to 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.[23] In July 2012, TSA expanded the program to include flight attendants.[24]

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 (SPOT) 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. Questions remain regarding the effectiveness of the behavioral detection program, 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 116th and earlier Congresses did

[20] Department of Homeland Security, Transportation Security Administration, Fiscal Year 2016 Congressional Justification, Aviation Security.

[21] Sheldon H. Jacobson, Arash Khatibi, and Ge Yu, "When Should TSA PreCheck Be Offered at No Cost to Travelers?" *Journal of Transportation Security,* 10, June 2017, pp. 23-39.

[22] Transportation Security Administration, *TSA Biometrics Roadmap*, September 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[23] See http://www.knowncrewmember.org/.

[24] Transportation Security Administration, *Press Release: U.S. Airline Flight Attendants to Get Expedited Airport Screening in Second Stage of Known Crewmember Program*, Friday, July 27, 2012, http://www.tsa.gov/press/releases/2012/07/27/us-airline-flight-attendants-get-expedited-airport-screening-second-stage.

not move to do so. The 116th and earlier Congresses also did not take specific action to revamp the program, despite concerns raised by GAO and the DHS Office of Inspector General.[25]

P.L. 115-254 directed TSA to utilize risk-based strategies in deploying federal air marshal teams on international and domestic flights. Air Marshals deploy under risk-based scheduling practices and must meet statutory obligations to cover all flights that are assessed as high-risk.[26] However, a more controversial TSA initiative using air marshals to shadow passengers whose behavioral profiles based on past itineraries indicated they might pose an elevated security risk was reportedly shuttered in December 2018 after media reports and some Members of Congress raised concerns over privacy implications of the program.[27]

The Use of Terrorist Watchlists in the Aviation Domain

Airlines were formerly responsible for checking passenger names against terrorist watchlists maintained by the government. The Intelligence Reform and Terrorist Prevention Act of 2004 (P.L. 108-458) mandated that DHS assume this function, but efforts to do so were significantly delayed by concerns regarding privacy and data protections. Following at least two instances in 2009 and 2010 in which passenger records checks failed to identify individuals who may pose 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 are being vetted using the Secure Flight system.[28]

Secure Flight vets passenger name records against a subset of the Terrorist Screening Database (TSDB). On international flights, Secure Flight operates in coordination with the use of watchlists by CBP's National Targeting Center-Passenger, which relies on the Advance Passenger Information System (APIS) 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 if they should receive expedited, standard, or enhanced screening at airport checkpoints.[29] Secure flight compares passenger records against the No-Fly and Selectee lists which are subsets of the TSDB used to identify individuals that should be denied boarding or subject to enhanced security screening. As the name implies, 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 lists of individuals who are to receive special scrutiny during pre-flight security screening and whose

[25] U.S. Government Accountability Office, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, GAO-14-159, November 2013; Department of Homeland Security, Office of Inspector General, *Transportation Security Administration's Screening of Passengers by Observation Techniques (Redacted)*, OIG-13-91, Washington, DC, May 29, 2013; Department of Homeland Security, Statement of Charles K. Edwards, Deputy Inspector General, Before the United States House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, November 13, 2013.

[26] See 49 U.S. Code § 44917.

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

[28] Department of Homeland Security, "DHS Now Vetting 100 Percent of Passengers on Flights Within or Bound For U.S. Against Watchlists," Press Release, November 30, 2010.

[29] Department of Homeland Security, Transportation Security Administration, "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.

carry-on bags and checked baggage are to be examined more thoroughly. The primary list of such individuals is referred to as the Selectee List or Automatic Selectee List to indicate that these individuals are to be automatically selected for enhanced screening. Enhanced screening may include measures such as pat-downs and chemical trace detection swabs to test for explosives residue. Passengers not on these lists may be randomly selected for enhanced screening, and passengers or baggage that trigger alarms during initial screening may also undergo these additional measures.Central issues surrounding the use of terrorist watchlists in the aviation domain that may be considered during the 117th Congress include

- the speed with which watchlists 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 watchlist checks;
- the adequacy of established protocols for providing redress to individuals improperly identified as potential threats; and
- the adequacy of coordination with international partners.[30]

In addition, there has been a growing interest in finding better ways to utilize watchlists to prevent terrorist travel, particularly travel of radicalized individuals seeking to join forces with foreign terrorist organizations such as the Islamic State (IS).

Following the January 6, 2021, security breach of the United States Capitol, there has been policy debate surrounding the potential inclusion of U.S. citizens and permanent residents who have engaged in domestic terrorism or anti-government violence on the No-Fly list.[31] Additionally, past airline actions to ban disruptive passengers, including passengers who have refused to comply with onboard masking requirements, have prompted debate about the desirability of replacing airlines' blacklists, which are not shared with other 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 mainly on international terrorist threats, and their possible use for these additional purposes may prompt congressional debate about whether an expansion of watchlists could divert TSA from its traditional focus.

Perimeter Security, Access Controls, and Worker Vetting

Airport perimeter security, access controls, and credentialing of airport workers are generally responsibilities of airport operators. 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.

[30] 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 upon request).

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

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.

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. State and local law enforcement agencies with jurisdiction at the airport 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").

TSA requires security background checks of airport workers with 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 include 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 offences, are disqualifying. Airports must collect applicant biographical information and fingerprints to submit to TSA to process background checks. P.L. 115-254 established more stringent standards for individuals applying for SIDA access, requiring that such individuals provide their social security number in order to strengthen vetting effectiveness. Many airports use a service known as the Transportation Security Clearinghouse to coordinate the processing of background check applications.[32] 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 (FBI's) Rap Back service. Additionally, TSA maintains a centralized database of individuals who have had security access or aircraft-operator credentials revoked for failing to comply with aviation security requirements as required by law.

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 be 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.

Explosives Screening Technology and Canines

Explosives screening technologies at passenger screening 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. TSA began introducing computed tomography (CT) scanning technology at passenger screening checkpoints in FY2018 on a trial basis, and procured additional units in FY2019 and FY2020 to expand the use of CT technology for scanning carry-on items. Through FY2020, TSA had deployed about 300 units at major airports. TSA asserts that CT technology offers automated capabilities to help improve detection of explosives and other threats.[33] TSA concedes, however, that the introduction of CT technology, at least initially, will

[32] See https://www.tsc-csc.com.

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

require more resources to clear increased numbers of false alarms compared to X-ray technology, and seeks to increase screener numbers at those airports where CT will be deployed to minimize these impacts on passenger screening. P.L. 115-254 directed TSA to proceed with these use of CT to screen both carry-on items and cargo carried on passenger aircraft. The act also directed TSA to assess other emerging screening technologies that may be used to enhance air cargo screening.

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

The TSA's National Explosives Detection Canine Team Program trains and deploys canines and 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, while 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 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 117th Congress may have interest in oversight of the third-party canine program to review 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 will typically not have a lead role in event response. However, federal law enforcement may assume a lead investigative role following a security incident, particularly if the event is determined to be an act of terrorism.

On January 17, 2017, a mass shooting 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. However, 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 117th Congress may consider whether such actions by individual airlines are acceptable.

P.L. 115-254 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.[34] The act also directed TSA to increase funding under the law enforcement reimbursable program for airports to increase the presence of law enforcement officers in public areas to provide visible deterrents to terrorists, including in baggage claim and ticketing areas and on airport access roads, as well as at screening checkpoints. TSA, however, has 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.

On November 1, 2013, a lone gunman targeting TSA employees fired several shots at a screening checkpoint at Los Angeles International Airport (LAX), killing one TSA screener and injuring two other screeners and one airline passenger. In a detailed postincident 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), named in honor of the TSA screener killed in the LAX incident and enacted in September 2015, requires 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 requires 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. P.L. 115-254 directed TSA to increase funding for the reimbursable program to expand protection of public areas of airports as well as screening checkpoints. Since past administrations have sought to reduce or restrict grant awards and reimbursements to airports for law enforcement and security functions, the 117th Congress may have interest in working with the Biden Administration to more clearly define federal roles and funding mechanisms for activities related to the security of public areas of airports.

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.[35] As part of this regulation, TSA inspects foreign airports from which commercial flights proceed directly to the United States. Officials known as Transportation Security Administration Representatives (TSARs) assess country compliance with international standards for aviation security and plan and coordinate U.S. airport risk analysis and assessments of foreign airports. TSARs also administer and coordinate TSA response to terrorist incidents and threats to U.S. citizens and transportation assets and interests overseas.

Sixteen foreign last point of departure airports (nine in Canada, two in the Bahamas, one in Bermuda, one in Aruba, two in Ireland, and one in Abu Dhabi) have CBP preclearance facilities where passengers are admitted to the United States prior to departure. Passengers arriving on

[34] Transportation Security Administration, *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.

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

international flights from these preclearance airports deplane directly into the airport sterile area upon arrival at the U.S. airport of entry, 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 and airports and reached agreements to offer preclearance at airports in Stockholm, Sweden, and Punta Cana, Dominican Republic, no additional preclearance locations have been established. TSA is also working to increase checked baggage preclearance processing so checked baggage does not have to be rescreened by TSA at the U.S. airport of entry, which has been the practice.

Congress in P.L. 114-190 required TSA to conduct security risk assessments at all last point of departure airports, and authorizes the donation of security screening equipment to such 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 satisfactorily demonstrate that they are capable of properly maintaining 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. Subsequently, however, the United States restricted scheduled air service and public charter flights between the United States and airports in Cuba other than José Martíi International Airport due to international policy concerns.[36]

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 soon after the 9/11 terrorist attacks 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 the threat was the multiyear Counter-MANPADS program carried out by the DHS Science & Technology Directorate. 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, however, due largely to high acquisition and life-cycle costs. U.S. airlines have not voluntarily invested in these systems for operational use, and argue that the costs for such systems should be borne, at least in part, by the federal government.

MANPADS are mainly seen as a security threat to civil aviation overseas, but a MANPADS attack in the United States could have a considerable impact on the airline industry. While major U.S. airports have conducted vulnerability studies, efforts to reduce vulnerabilities to potential MANPADS attacks face significant logistic challenges. While Congress has not formally debated the issue since the conclusion of the DHS program in 2009, any future terrorist attempts to use standoff weapons, including shoulder-fired missiles, to attack civilian aircraft could quickly escalate this to a major national security priority.

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

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 to 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 117th Congress may have an interest in policies and technologies to mitigate safety and security threats posed by unmanned aircraft.

Terrorists could potentially 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 even 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 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 United Nations General Assembly, causing damage to one of the helicopter's rotor blades.

Numerous other safety incidents involving drones have been reported in the United States and abroad; few have been tied to terrorism. ISIS is known to have used small drones in conflict zones to conduct reconnaissance and drop explosives. While the payload capacities of small unmanned aircraft would likely limit the damage a terrorist attack using conventional explosives could inflict, drone attacks using chemical, biological, or radiological weapons could be more serious.

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.[37] This requirement does not apply to recreational users, who are already permitted to operate small drones at low altitudes. While FAA has issued general guidance to law enforcement regarding unlawful UAS operations,[38] it is not clear that law enforcement agencies have sufficient training or technical capacity to respond to this potential threat.[39]

Technology may help manage security threats posed by unmanned aircraft. Integrating tracking mechanisms as well as incorporating "geo-fencing" capabilities, designed to prevent flights over sensitive locations or in excess of certain altitude limits, into unmanned aircraft systems may help curtail unauthorized flights.[40]

Congress in P.L. 114-190 directed FAA to establish a pilot program to detect and mitigate unmanned aircraft operations in the vicinity of airports and other critical infrastructure.

---

[37] See 14 C.F.R. §61.18.

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

[39] Statement of Chief Richard Beary, President of the International Association of Chiefs of Police, Subcommittee on Oversight and Management Efficiency, Committee on Homeland Security, U.S. House of Representatives, March 18, 2015.

[40] See, e.g., Todd Humphreys, "Statement on the Security Threat Posed by Unmanned Aerial Systems and Possible Countermeasures," Submitted to the Subcommittee on Oversight and Management Efficiency, House Committee on Homeland Security, March 16, 2015.

Additionally, the act directed FAA to develop an air traffic management system for small UASs that could include measures to detect and deter security threats posed by UASs.

In January 2021, FAA issued regulations that require drones to be equipped with remote identification capabilities that continually broadcast position and identification information or restrict operations to specified areas like airparks designated for remote-controlled model aircraft.[41] These requirements are to be phased in, requiring newly manufactured UAS to come equipped with such capabilities by September 2022, and all UAS including existing drones to comply with operational requirements by September 2023.

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 a UAS to certain security-related facilities in the United States. The act authorizes the military to detect, monitor, and track UASs; issue warnings to operators; disrupt control of a UAS, including interrupting or jamming control signals; seize or take control of the UAS; confiscate the unmanned aircraft; or use reasonable force to disable or destroy the UAS. P.L. 115-254 more broadly authorizes the Department of Justice and DHS to take similar defensive actions to protect people, facilities, or assets from credible threats posed by UASs. The act also expands 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 unmanned aircraft.

P.L. 115-254 also directed FAA to coordinate with the various agencies authorized to engage in counter-unmanned aircraft (C-UAS) activities and work with these agencies to ensure that technologies developed to mitigate risks posed by an 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 arming unmanned aircraft with dangerous weapons. Additionally, the act establishes 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, or other buildings or grounds hosting a special event of national significance. It also establishes criminal penalties for using a drone in a manner that interferes with wildfire suppression efforts or related law enforcement or emergency response activities. The 117th Congress may have interest in reviewing the adequacy and effectiveness of existing statutes pertaining to drone uses that pose a security risk and the legal framework for counter-UAS measures to detect and interdict such operations.

Aviation Cybersecurity

There is growing concern over cybersecurity threats to aircraft, air traffic control systems, and airports. Executive Order 13636 provides broad guidance for DHS to work with FAA to identify cybersecurity risks, establish voluntary cybersecurity measures, and share information on cybersecurity threats within the broader cybersecurity framework. Additionally, Congress in statute has specifically directed TSA to periodically review threats to civil aviation with a particular focus on specified threats, including the potential disruption of civil aviation service resulting from a cyberattack.[42]

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

[42] See 49 U.S.C. §44912.

TSA has indicated that its approach to cybersecurity thus far has not been through regulation, but rather through voluntary collaboration with industry. TSA's 2018 Cybersecurity Roadmap identities top strategic priorities for cybersecurity which include

- assessing and prioritizing evolving cybersecurity risks to TSA and transportation sector systems;
- reducing vulnerabilities through protective and preventive measures;
- mitigating consequences though coordinated response efforts;
- strengthening security and resilience of the cyber environment across the transportation sector; and
- promoting collaborative efforts to improve management of cybersecurity activities.[43]

In recognition of persisting cybersecurity threats, particularly to air traffic and air navigation systems and other critical cyber components of the national airspace system, FAA has developed a software assurance policy for all FAA-owned and FAA-controlled information systems.[44] While FAA has adopted an evolving framework to address the cybersecurity of its systems, a January 2018 GAO report warned that new aircraft tracking technologies that will transform air traffic control in the coming years under NextGen have unmitigated cybersecurity vulnerabilities, including vulnerabilities to jamming, hacking, and spoofing of signals, that could compromise air traffic operations as well as pose a threat to national security and military aircraft operations.[45]

For systems onboard aircraft, FAA requires cybersecurity to be addressed in the existing airworthiness certification process. Large commercial aircraft and aviation systems manufacturers now typically collaborate with software security companies to attain high levels of assurance for software embedded in avionics equipment. Despite efforts to design aircraft systems to be resilient to cyberthreats, in April 2015, TSA and the FBI issued warnings that the increasing interconnectedness of these systems makes them vulnerable to unauthorized access.[46] TSA and FBI advised airlines to look out for individuals trying to tap into aircraft electronics and for evidence of tampering or network intrusions.

Language in P.L. 114-190 mandated development of a comprehensive strategic framework for reducing cybersecurity risks to the national airspace system, civilian aviation, and FAA information systems. P.L. 115-254 directed FAA to review and update that framework to address known cybersecurity risks to the aviation system and short-term and long-term objectives for addressing these risks. It also ordered a National Academy of Sciences study to develop recommendations on how to increase the size, quality, and diversity of FAA's cybersecurity workforce. The act also directed FAA to address cybersecurity in the certification of aircraft avionics systems and component software, and the cybersecurity of systems and technologies relating to the air traffic control system. The act also directed FAA to develop an integrated cybersecurity testbed for air traffic control modernization technologies. FAA has developed the

[43] Transportation Security Administration, *TSA Cybersecurity Roadmap 2018,* November 1, 2018, https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap_adm_approved.pdf.

[44] Federal Aviation Administration, "Order 1370.109: National Policy, Software Assurance Policy," effective October 23, 2009.

[45] Government Accountability Office, *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft,* GAO-18-177, January 2018.

[46] Kim Zetter, "Feds Warn Airlines to Look Out for Passengers Hacking Jets," *Wired,* April 21, 2015, http://www.wired.com/2015/04/fbi-tsa-warn-airlines-tampering-onboard-wifi/.

National Airspace (NAS) System Cyber Engineering Facility and NAS Cyber Monitoring System to assess cyber threats and vulnerabilities and conduct cyber testing and evaluation.[47] It has also joined forces with DHS and the Department of Defense to coordinate development of the strategic framework for civil aviation cybersecurity under a joint agency Aviation Cyber Initiative.[48]

P.L. 115-254 directed TSA to implement the framework for improving critical infrastructure cybersecurity developed by the National Institute of Standards and Technology to manage cybersecurity risks. It also instructed TSA to conduct cybersecurity vulnerability assessments, including cybersecurity evaluations of the PreCheck program and transportation worker credentialing programs that contain data on individuals. The act also directed TSA to coordinate with international counterparts to harmonize validation processes, allowing reciprocal recognition of security and screening technology approvals that comply with agreed-upon standards relating to performance as well as information security and cybersecurity. The act also directed DHS to review global aviation security standards and practices, including assessments of the cybersecurity risks of security screening equipment.

In November 2018, TSA released a new cybersecurity roadmap providing a broad framework for how it will work with transportation industry and government stakeholders to address cybersecurity risks, including risks to aviation.[49] The specific roles of TSA and FAA in regulating cybersecurity, particularly in areas such as aircraft and avionics certification and air traffic control, which have historically been FAA responsibilities, may be a topic for congressional oversight during the 117th Congress.

Transit and Passenger Rail Security[50]

Bombings of and shootings on passenger trains in Europe and Asia have illustrated the vulnerability of passenger rail systems to terrorist attacks. Passenger rail systems—primarily subway systems—in the United States carry about five times as many passengers each day as do airlines, over many thousands of miles of track, serving stations that are designed primarily for easy access. The increased security efforts around air travel have led to concerns that terrorists may turn their attention to "softer" targets, such as transit or passenger rail. A key challenge Congress faces is weighing the desire for increased rail passenger security; the efficient functioning of transit systems; the potential costs and damages of an attack; and other federal priorities.

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. Consequently, transit security measures tend to emphasize managing the consequences of an attack. Nevertheless, steps have been taken to try to reduce the risks of an attack as well. These include

- vulnerability assessments;
- emergency planning;
- emergency response training and drilling of transit personnel (ideally in coordination with police, fire, and emergency medical personnel);

[47] See https://www.faa.gov/air_traffic/technology/cas/ct/.

[48] See https://www.faa.gov/air_traffic/technology/cas/aci/.

[49] Transportation Security Administration, *TSA Cybersecurity Roadmap 2018,* https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap_adm_approved.pdf.

[50] This section was prepared by David Randall Peterman, Analyst in Transportation Policy.

- increasing the number of transit security personnel;
- installing video surveillance equipment in vehicles and stations; and
- conducting random inspections of bags, platforms, and trains.

The challenges of securing rail passengers are dwarfed by the challenge of securing bus passengers. There are typically some 76,000 buses carrying 19 million passengers each weekday in the United States (passenger numbers declined in 2020 due to the pandemic). Some transit systems have installed video cameras on their buses, but the number and operating characteristics of transit buses make them all but impossible to secure.

In contrast with the aviation sector, where TSA provides security directly, security in surface transportation is provided primarily by the transit and rail operators and local law enforcement agencies. TSA's main roles are oversight, coordination, intelligence sharing, training, and assistance. However, it 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." Several presidential Administrations have sought to reduce the size of the VIPR program, the value of which has yet to be demonstrated,[51] but prior Congresses sought to increase the size of the program.

Congressional efforts to promote the security of passenger rail and transit include providing grants to service providers, requiring those providers considered to be high-risk targets (by DHS) to have 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 three primary objectives for reducing risk in transit are to

- increase system resilience by protecting high-risk/high-consequence assets (i.e., critical tunnels, stations, and bridges);
- expand visible deterrence activities (i.e., canine teams, passenger screening teams, and antiterrorism teams); and
- engage the public and transit operators in the counterterrorism mission.[52]

TSA surface transportation security inspectors conduct assessments of transit systems (and other surface modes) through the agency's Baseline Assessment for Security Enhancement (BASE) program. The agency has also developed a security training and security exercise program for transit. TSA's program for securing surface transportation is known as Risk Mitigation Activities for Surface Transportation (RMAST).

The intent of the RMAST program is to focus TSA's limited surface security resources on high-risk entities and locations. GAO reported in 2017 that TSA had not identified or prioritized high-risk entities for the RMAST program to focus on.[53]

The surface transportation inspector program has been a focus of congressional interest. Issues of concern to Congress have included

[51] Department of Homeland Security, 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.

[52] Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2016 Congressional [Budget] Justification*, p. 11.

[53] Government Accountability Office, *Transportation Security Administration: Surface Transportation Inspector Activities Should Align More Closely With Identified Risks*, GAO-18-180, December 2017, p. 30.

- whether the inspectors promoted from screening passengers at airports have sufficient expertise in surface transportation security;
- the administrative challenge of having the surface inspectors managed by airport-based federal security directors who themselves typically have no surface transportation experience; and
- the security value of the tasks performed by surface inspectors.[54]

The number of surface inspectors declined from 404 in FY2011 to 290 (full-time equivalent positions) in FY2020. TSA attributed the decrease to efficiencies achieved through focusing efforts on the basis of risk.[55] However, in 2017 GAO reported that surface transportation inspectors were spending more time on the surface transportation mode that TSA had identified as the lowest risk than on the one identified as the highest risk (for security reasons, these modes were not identified).[56] Surface inspection field offices are located near airports, and surface inspectors may spend a significant portion of their time on tasks related to aviation safety, but TSA does not have complete information on the extent to which surface inspectors are tasked to work on aviation security.[57]

GAO reported in 2014 that lack of guidance to TSA's surface inspectors resulted in inconsistent reporting of rail security incidents and that TSA had not consistently enforced the requirement that rail agencies report security incidents, resulting in poor data on the number and types of incidents.[58] GAO also found that TSA did not have a systematic process for collecting and addressing feedback from surface transportation stakeholders regarding the effectiveness of its information-sharing effort.[59] In a 2015 hearing, GAO testified that TSA had put processes in place to address these issues.[60]

DHS provides grants for security improvements for public transit, passenger rail, and occasionally other surface transportation modes under the Transit Security Grant Program (see **Table 1**). The vast majority of the funding goes to public transit providers. Funding for these grant programs is an ongoing issue of interest to the 117th Congress with respect to annual appropriations for these activities as well as their relationship to other DHS programs.

---

[54] U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, Hearing on *TSA's Surface Inspection Program: Strengthening Security or Squandering Resources?*, May 31, 2012, http://homeland.house.gov/hearing/subcommittee-hearing-tsa%E2%80%99s-surface-inspection-program-strengthening-security-or-squandering.

[55] Peter Neffenger, Administrator, Transportation Security Administration, U.S. Department of Homeland Security, *Statement to the United States Senate Committee on Commerce, Science, and Transportation,* Hearing on Transportation Security, April 6, 2016; Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2014 Congressional [Budget] Justification*, p. 14.

[56] Government Accountability Office, *Transportation Security Administration: Surface Transportation Inspector Activities Should Align More Closely With Identified Risks*, GAO-18-180, December 2017, pp. 24-26.

[57] Ibid., p. 20: Several surface inspectors estimated spending 20%-50% of their work time on aviation tasks.

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

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

[60] Government Accountability Office, *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, given before the U.S. House of Representatives, Committee on Homeland Security, Subcommittees on Transportation Security and Counterterrorism & Intelligence, September 17, 2015.

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 public transportation security grant program.[61] Despite this finding, earlier Congresses have not supported consolidation of the programs, though some congressional appropriators have expressed concern that grant programs have not focused on areas of highest risk and that significant amounts of previously appropriated funds have not yet been awarded to recipients.

Table 1. Congressional Funding for Transit Security Grants, FY2002-FY2020

Fiscal Year	Appropriation (millions of nominal dollars)	Appropriation (millions of 2020 dollars)
2002	$63[a]	$89
2003	65	90
2004	50	68
2005	108	142
2006	131	167
2007	251	311
2008	356	427
2009	498[b]	597
2010	253	298
2011	200	231
2012	88[c]	99
2013	84	93
2014	90	98
2015	87	95
2016	87	94
2017	88	94
2018	88	92
2019	88	90
2020	88	88

Source: FY2002: Department of Defense FY2002 Appropriations Act, P.L. 107-117; FY2003: FY2003 Emergency Wartime Supplemental Appropriations Act, P.L. 108-11; FY2004: Department of Homeland Security FY2004 Appropriations Act, P.L. 108-90; FY2005-FY2011: 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; FY2012-2020: DHS, Transit Security Grant Program annual funding opportunity announcements.

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 2020 dollars using the Total Non-defense column from Table 10: Gross Domestic Product and Deflators Used in the Historical Tables: 1940-2025, published in the Historical Tables volume of the Budget of the United States Government, Fiscal Year 2021 (https://www.whitehouse.gov/omb/historical-tables/).

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

[61] United States Government Accountability Office, *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, GAO-12-303, February 2012.

b. Includes $150 million provided in the American Recovery and Reinvestment Act.
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.

In P.L. 114-50, Congress directed TSA to ensure that all passenger transportation providers it considers as having high-risk facilities have in place plans to respond to active shooters, acts of terrorism, or other security-related incidents that target passengers. TSA efforts to ensure that these requirements have been met may be of interest for congressional oversight in the 117th Congress.

Port and Maritime Security[62]

The bulk of U.S. overseas trade is carried by ships, and thus the economic repercussions of a maritime terrorist attack could be significant. In the aftermath of the 9/11 attacks, the U.S. Customs Service (now Customs and Border Protection, CBP) and the Coast Guard realized that they needed to "push the borders out"—that is, they needed to begin screening vessels and cargo before they reached a U.S. port. While the previous screening methods that occurred at U.S. ports were sufficient to intercept other illicit cargo (e.g., drug smuggling) they could be too late in the case of intercepting a terrorist bomb. Thus, Customs instituted the "24-hour rule," requiring importers to submit shipment information to Customs (now CPB) a day before the shipment arrived 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 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.)

Similarly, the Coast Guard recognized the need to extend terrorist screening beyond U.S. ports. It required ships to announce and report their intended arrival four days before entering a U.S. harbor. The Coast Guard examines the vessel's particulars, its crew, and past history to evaluate the security risk. The Coast Guard pushed 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.

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 that 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. The Coast Guard recognizes that U.S. ports vary greatly in terms of their geographies and types of cargo they handle. The port security plans allow the industry to develop plans specific to their vulnerabilities. An important

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

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, along with TSA, has also instituted a port worker background check for longshoremen, truck drivers, vessel crews, and others that need access to port terminals. A Transportation Worker Identification Credential (TWIC) card must be obtained from the TSA and renewed every five years.

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 (SAFE Port Act; P.L. 109-347). Congress modified these maritime security programs in Division J of the FAA Reauthorization Act of 2018 (P.L. 115-254).

Recent cyberattacks on container shipping lines has focused attention on cyber vulnerabilities in the maritime industry. 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. A less severe attack affected COSCO Shipping in July 2018 and Mediterranean Shipping Company in April 2020. A cyberattack on CMA CGM container line in September 2020 also affected its ability to accept cargo bookings. In addition to ports and shipping lines that use computer networks to book and track cargo, the development of electronic navigation ("e-navigation"), involving the replacement of paper charts with electronic charts (already commonplace) or the replacement of channel marker buoys with virtual aids to navigation (in progress), could create vulnerabilities to cyberattack. P.L. 115-254 incorporated cybersecurity as a required element in MTSA security plans for terminal and vessel operators. The Coast Guard has provided guidance for vessels and ports to address cyber vulnerabilities, and has incorporated cybersecurity into existing enforcement and compliance programs.[63] The Coast Guard has added cybersecurity training to the requirements for mariner licensing and for port security officer qualifications. In October 2020, the Department of Energy announced that it was developing guidelines for the maritime components of the energy industry to protect against cyberattacks.[64]

A provision in the National Defense Authorization Act for FY2021 (NDAA, P.L. 116-283, Section 8244) requires the Coast Guard to report on its response capabilities to cyber incidents on U.S.-flag vessels. Section 9003 of the FY2021 NDAA requires DHS to review and report to Congress on CBP operations with respect to the screening of international cargo at Great Lakes and inland ports and provide a separate report analyzing security threats at inland ports.

Security at Land Border Ports of Entry[65]

Section 9007 of the FY2021 NDAA requires DHS to submit a plan for scanning all incoming vehicles crossing the Canadian and Mexican borders with large-scale non-intrusive inspection equipment, to include passenger cars, trucks, and railcars. This equipment must be capable of producing an image of the contents of the vehicle, such as by x-ray or gamma ray. Currently, this

[63] Coast Guard, Navigation and Vessel Inspection Circular (NVIC) 01-20; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, February 26, 2020; https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023.

[64] Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response, "Department of Energy Invests $3 million to enhance U.S. energy and maritime industries' cybersecurity capabilities," October 5, 2020.

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

equipment is mostly used by CBP at secondary vehicle inspection stations after a CBP official has determined that a more intrusive inspection is warranted at the primary inspection station.[66] Most vehicles are also inspected by passive radiation portal monitors as they pass through the primary inspection station. The strategy of attempting to produce an image of the contents of 100% of the vehicles entering the United States is controversial because of the time and cost of both producing the image and analyzing the image for security risks. At seaports, such imaging systems have been determined to be infeasible for inspecting 100% of imported containers. Some argue that the resources devoted to 100% imaging, such as analyzing the images of the vast number of vehicles not presenting a security risk, could be better applied to identifying those vehicles that present higher or unknown security risks. In December 2019, a CBP official testified that at the Mexican border, CBP scans less than 2% of private vehicles and 15% of commercial vehicles, but had expected to increase these percentages to 40% and 72%, respectively, by FY2023.[67]

Author Information

Bart Elias
Specialist in Aviation Policy

David Randall Peterman
Analyst in Transportation Policy

John Frittelli
Specialist in Transportation Policy

Disclaimer

[66] CRS Report R43014, *U.S. Customs and Border Protection: Trade Facilitation, Enforcement, and Security*, by Vivian C. Jones and Audrey Singer.

[67] Testimony of Hector Mancha, CBP Director of Field Operations at El Paso, House Committee on Homeland Security, Subcommittee on Oversight, Management, and Accountability, "Promoting Safe and Efficient Travel and Trade at America's Land Ports of Entry," December 2, 2019.