Transportation Security: Issues for the 116th Congress

February 11, 2019

Congressional Research Service
https://crsreports.congress.gov
R45500

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Transportation Security: Issues for the 116th Congress

SUMMARY

R45500

February 11, 2019

Bart Elias
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

David Randall Peterman
Analyst in Transportation Policy

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, the 107th 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 the extensive focus on aviation and transportation security over the past decade, 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
- 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 the passenger screening process, mandate more rigorous background checks of airport workers, strengthen airport access controls, increase passenger checkpoint efficiency and operational performance, 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 116th Congress. Particular topics may include the evolution of screening technologies and assessments of emerging screening technology solutions; the expansion of canine teams for transportation security; 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 using drones.

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

Introduction 1
Aviation Security 1
- Explosives Screening Strategy for the Aviation Domain 2
- Risk-Based Passenger Screening 4
- The Use of Terrorist Watchlists in the Aviation Domain 7
- Perimeter Security, Access Controls, and Worker Vetting 8
- Explosives Screening Technology and Canines 9
- Protecting Public Areas of Airports 10
- Foreign Last Point of Departure Airports 10
- Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft 11
- Security Issues Regarding the Operation of Unmanned Aircraft 12
- Aviation Cybersecurity 14

Transit and Passenger Rail Security 16
Port and Maritime Security 20

Tables

Table 1. Congressional Funding for Transit Security Grants, FY2002-FY2018 19

Contacts

Author Information 22

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 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.

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 an attack from within a transportation system, such as occurred on September 11, 2001. The concern is that attackers could once again disguise themselves as legitimate passengers (or shippers or workers) to get in position 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 took swift action to create the Transportation Security Administration (TSA) within the U.S. Department of Transportation and gave 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]

To this day, 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.[3] 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

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

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

[3] Transportation Security Administration, *Screening Partnership Program*, http://www.tsa.gov/stakeholders/screening-partnership-program.

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 extensive focus on 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 standoff weapons; 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. 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 closely 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 pre-departure vetting.

P.L. 115-254 requires 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 requires U.S. Customs and Border Protection to work with TSA to establish a formal ACAS program for inbound international cargo modelled on the long-running ACAS pilot program. It directs TSA to examine the feasibility of expanding the use of computed tomography to air cargo and examine other emerging screening technologies that may enhance air cargo screening.

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 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 requires TSA to update this plan annually to accompany its budget request. The act also requires 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.

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,[4] 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 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.[5] 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.

The use of AIT has raised a number of policy questions. Privacy advocates have objected to the intrusiveness of AIT, particularly when used for primary screening.[6] 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

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

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

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

generally not considered harmful. More recently, the effectiveness of AIT and ATR has 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.[7]

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 FY2018, TSA deployed about 960 AIT units. It has not planned for procurements beyond this level, although many smaller airports are not equipped with this capability. 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, likewise, is not available at many smaller airports: Currently, the program's incentive of expedited screening is offered at fewer than half of all commercial passenger airports.

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 instructs 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 directs TSA to promote a diverse security technology industry to better enable small business innovators to develop and commercialize new transportation security technologies. The act requires TSA to formally establish its innovation task force to accelerate the development of innovative transportation security technologies and capabilities. The act also directs DHS to conduct a review to determine whether the Transportation Security Laboratory 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 Directorate for more than a decade.

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.

[7] 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.

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 2018, 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.

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.[8]

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. The Government Accountability Office (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.[9]

TSA phased out the managed inclusion program in the fall of 2015. Since September 2015, TSA behavior detection officers and explosives trace detection personnel no longer direct passengers 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. TSA has estimated annual savings in direct screener workforce costs totaling $110 million as a result of PreCheck and other risk-based initiatives.[10] A 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 to 20 million.[11] PreCheck expansion was addressed in recent legislation[12] and oversight of TSA efforts to expand PreCheck may be a specific topic of interest during the 116th Congress.

Language in P.L. 115-254 directs TSA to work with at least two private-sector entities to expand PreCheck enrollment options and forge at least two agreements for marketing the program, setting enrollment targets of 7 million by the end of FY2019, 10 million by the end of FY2020, and 15 million by the end of FY2021. The act also directs TSA to explore cost-effective options for conducting recurrent background checks of program participants, although this could raise

[8] 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.

[9] 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.

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

[11] 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.

[12] See P.L. 114-190 and P.L. 115-254.

concerns over impacts on enrollments if procedures for recurrent checks impose additional burdens on participants.

The act requires 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 instructs 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 directs 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,[13] 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 congressional oversight committees.

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.[14] In July 2012, TSA expanded the program to include flight attendants.[15]

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, Congress has not moved to do so. For example, H.Amdt. 127 (113th Congress), an amendment to the FY2014 DHS appropriations measure that sought to eliminate funding for the program, failed to pass a floor vote. Congress also has not taken specific action to revamp the program, despite the concerns raised by GAO and the DHS Office of Inspector General.[16]

P.L. 115-254 directed TSA to utilize risk-based strategies in deploying federal air marshal teams on international and domestic flights. 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

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

[14] See http://www.knowncrewmember.org/Pages/Home.aspx.

[15] 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.

[16] 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.

reports and some Members of Congress raised concerns over the privacy implications of the program.[17]

The Use of Terrorist Watchlists in the Aviation Domain

Airlines were formerly responsible for checking passenger names against terrorist watchlists maintained by the government. Following at least two instances in 2009 and 2010 in which such 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.[18]

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 in-bound 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 carried out by the airlines through use of the Computer-Assisted Passenger Prescreening System (CAPPS). In January 2015, TSA gave notification that it would start incorporating the results of CAPPS assessments, but not the underlying data used to make such assessments, into Secure Flight, along with each passenger's full name, date of birth, and PreCheck traveler number (if applicable). These data are used within the Secure Flight system to perform risk-based analyses to determine whether passengers receive expedited, standard, or enhanced screening at airport checkpoints.[19] P.L. 115-254 removed statutory references to CAPPS, replacing them with references to the Secure Flight Program to clarify that these various passenger vetting elements are fully encompassed under Secure Flight. The act also directed TSA to conduct and publicly disseminate a review of its privacy impact assessment of the Secure Flight Program.

Central issues surrounding the use of terrorist watchlists in the aviation domain that may be considered during the 116th 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.[20] 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).

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

[18] 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.

[19] 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.

[20] 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.

Language in P.L. 114-190 directed TSA to assess whether recurrent fingerprint-based criminal background checks could be carried out in a cost-effective manner to augment terrorist watchlist checks for PreCheck program participants. Additionally, the act directed TSA to expand criminal background checks for certain airport workers.

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.

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 from intrusion, including buildings and terminal areas. 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. Many airports use a service known as the Transportation Security Clearinghouse to coordinate the processing of background check applications.[21]

P.L. 114-190 directed TSA to update the eligibility criteria and disqualifying criminal offenses for SIDA access credentials based on other transportation vetting requirements and knowledge of insider threats to security. The law proposes that TSA expand the criminal history look-back period from the current 10 years to 15 years, and that individuals be disqualified if they have been released from prison within 5 years of their application. The statute directs TSA to establish a formal waiver process for individuals denied credentials. It also calls for full implementation of recurrent vetting of airport workers with SIDA access credentials using the Federal Bureau of Investigation's (FBI's) Rap Back service to identify disqualifying criminal offences. Language in P.L. 115-254 requires TSA to provide congressional oversight committees with data on the number of airport workers being continuously vetted though the Rap Back service. It also directs TSA to identify means of using homeland security and intelligence resources to educate TSA personnel on means to better mitigate insider threats. The law also requires TSA to establish a centralized database of individuals who have had security access or aircraft-operator credentials revoked for failing to comply with aviation security requirements.

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

P.L. 114-190 directed TSA to conduct random physical inspections of airport workers at SIDA access points and in SIDA areas. P.L. 115-254 clarifies 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 directs 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. The act also establishes more stringent standards for individuals applying for SIDA access, requiring that such individuals provide their social security number in order to strengthen vetting effectiveness.

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 plans to expand the use of CT technology for scanning carry-on items throughout FY2019, with an aim of deploying more than 150 units at 14 major airports. TSA asserts that CT technology offers automated capabilities to help improve detection of explosives and other threats.[22] TSA concedes, however, that the introduction of CT technology, at least initially, will 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 directs TSA to proceed with these CT pilot programs and also to examine the feasibility of using CT technology to screen cargo carried on passenger aircraft. The act also directs 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 370 TSA teams and 675 state and local law enforcement teams trained by TSA under partnership agreements. More than 350 of the TSA teams are dedicated to passenger screening at 46 airports. Following airport bombings in Brussels, Belgium, and Istanbul, Turkey, in 2016, there has been interest in increasing deployments of canine teams in non-sterile areas of airport terminals. P.L. 114-190 authorized TSA to provide training to foreign governments in airport security measures including the use of canine teams. The act also directed TSA to utilize canine teams to minimize passenger wait times and maximize security effectiveness of checkpoint operations.

P.L. 115-254 directs TSA to establish a working group to assess ways to support a decentralized, non-federal domestic breeding program for explosives detection canines and to modernize canine

[22] 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.

breeding, medical, technical, and training standards. It further instructs 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 that do not have their full allocation of explosives detection canine teams would be able to directly acquire canines from TSA approved third-party sources, but canines procured in this manner would be trained by TSA personnel. Additionally, the act directs TSA to issue standards for the primary screening of air cargo by private entities using dogs and handlers not owned or employed by TSA.

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.

P.L. 115-254 directs TSA to establish a working group to collaborate with public and private stakeholders to develop non-binding recommendations for enhancing security in public areas of transportation facilities. The act also directs 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.

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 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), 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, and P.L. 115-254 directs TSA to increase funding for the reimbursable program to expand protection of public areas of airports as well as screening checkpoints.

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.[23] 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.

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

TSARs also administer and coordinate TSA response to terrorist incidents and threats to U.S. citizens and transportation assets and interests overseas.

Fifteen foreign last point of departure airports (eight in Canada, two in the Bahamas, one in Bermuda, one in Aruba, two in Ireland, and one in Abu Dhabi) have Customs and Border Protection (CBP) preclearance facilities where passengers are admitted to the United States prior to departure. Passengers arriving on 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. CBP has announced its intention to expand customs preclearance to additional countries and airports. While agreements to offer preclearance at airports in Stockholm, Sweden, and Punta Cana, Dominican Republic, were finalized in 2016, preclearance operations at these airports have not yet been established. Plans to offer preclearance at other airports are still being negotiated.[24] Assessing screening measures at preclearance airports is a particular priority for TSA. 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.

Language in 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 airports to mitigate security vulnerabilities that put U.S. citizens at risk. P.L. 115-254 mandates 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. The act also directs DHS, in coordination with the Department of State, to review and improve international aviation security standards and dissemination and implementation processes for security directives and emergency amendments to security requirements issued to domestic and foreign air carriers. It instructs TSA to work with the International Civil Aviation Organization to raise minimum standards for aviation security. P.L. 115-254 also directs TSA to work with FAA to track public charter flights between the United States and Cuba, and to brief congressional oversight committees on aviation security measures at Cuban airports that have air service to the United States.

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

[24] U.S. Customs and Border Protection, *Preclearance Locations*, https://www.cbp.gov/border-security/ports-entry/operations/preclearance.

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.

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 116th Congress may have a particular 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 September 2011, the FBI disrupted a homegrown terrorist plot to attack the Pentagon and the Capitol with large model aircraft packed with high explosives.

Widely publicized drone incidents include an unauthorized flight at a political rally in Dresden, Germany, in September 2013 that came in close proximity to German Chancellor Angela Merkel; a January 2015 crash of a small hobby drone on the White House lawn in Washington, DC; a series of unidentified drone flights over landmarks and sensitive locations in Paris, France, in 2015; and drone sightings around London Gatwick and Heathrow airports in December 2018 that grounded numerous airline flights. These incidents have raised additional concerns about safety and security threats posed by small unmanned aircraft.

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, but few have been tied to terrorism. However, ISIS is known to have used 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.[25] However, this

[25] See 14 CFR §61.18.

requirement does not apply to recreational users, who are already permitted to operate small drones at low altitudes. Moreover, while FAA has issued general guidance to law enforcement regarding unlawful UAS operations,[26] it is not clear that law enforcement agencies have sufficient training or technical capacity to respond to this potential threat.[27]

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.[28]

Language 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. 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.

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 directs FAA to coordinate with the various agencies authorized to engage in counter-unmanned aircraft (C-UAS) activities to review standards, policies, and practices with respect to maintaining safety for airspace users, protecting individuals and property on the ground, and not interfering with avionics, navigation, and air traffic control systems. Additionally, the review is to assess the adequacy of those agencies' coordination with FAA regarding C-UAS operations, the adequacy of training for personnel operating C-UAS systems, information sharing regarding airspace authorizations, and best practices for consistent C-UAS operations. The act directs FAA to work with the Department of Defense (DOD), DHS, and other relevant agencies to ensure that technologies developed to mitigate risks posed by an errant or hostile UAS do not adversely impact safe airport operations and air traffic and air navigation services. The act also directs FAA to work with DOD to streamline deployment of C-UAS and requires FAA to develop a comprehensive strategy for identifying and responding to public safety threats posed by UASs. It also requires FAA to implement a pilot program using remote detection capabilities to identify UASs in order to carry out enforcement actions against UAS operators not in compliance with applicable aviation laws and regulations.

P.L. 115-254 establishes a formal prohibition against civilians arming unmanned aircraft with dangerous weapons. Additionally, the act establishes criminal penalties for flying a drone over the

[26] Federal Aviation Administration, *Law Enforcement Guidance for Suspected Unauthorized UAS Operations*, http://www.faa.gov/uas/regulations_policies/media/FAA_UAS-PO_LEA_Guidance.pdf.

[27] 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.

[28] 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.

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.

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, 49 U.S.C. §44912 specifically directs 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.

TSA has indicated that its approach to cybersecurity thus far has not been through regulation, but rather through voluntary collaboration with industry. Under this framework, TSA formed the Transportation Systems Sector Cybersecurity Working Group, which created a cybersecurity strategy for the transportation sector in 2012.[29] Also, in coordination with the FBI and industry partners, TSA launched the Air Domain Intelligence Integration Center and an accompanying analysis center in 2014 to share information and conduct analysis of cyberthreats to civil aviation.[30]

In recognition of those threats, FAA has developed a software assurance policy for all FAA-owned and FAA-controlled information systems.[31] However, according to an April 2015 GAO report, while FAA has taken steps to protect air traffic control systems from cyberthreats, it faces continuing challenges in mitigating cyberthreats, particularly as it transforms air traffic control systems under its NextGen modernization initiative.[32] 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.[33]

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

[29] Department of Homeland Security, "Executive Order 13636—Improving Critical Infrastructure Cybersecurity, Section 10(b) Report: TSA's Approach to Voluntary Industry Adoption of the NIST Cybersecurity Framework," http://www.dhs.gov/sites/default/files/publications/ExecutiveOrder_13636Sec10%28b%29Reportv5.pdf.

[30] Rachael King, "Aviation Industry and Government to Share Cyber Threats in New Intelligence Center," *Wall Street Journal CIO Journal*, April 15, 2014, http://blogs.wsj.com/cio/2014/04/15/aviation-industry-and-government-to-share-cyberthreats-in-new-intelligence-center/.

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

[32] Government Accountability Office, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to NextGen*, GAO-15-370, April 2015.

[33] 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.

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 and advised airlines to look out for individuals trying to tap into aircraft electronics and for evidence of tampering or network intrusions.[34]

FAA separately addresses cybersecurity of government-owned air traffic control systems and certified aircraft systems. However, GAO has cautioned that FAA's current approach to cybersecurity does not adequately address the interdependencies between aircraft and air traffic systems, and consequently may hinder efforts to develop a comprehensive and coordinated strategy.[35] While it identified no easy fix, GAO recommended that FAA develop a comprehensive cybersecurity threat model, better clarify cybersecurity roles and responsibilities, improve management security controls and contractor oversight, and fully incorporate National Institute of Standards and Technology information security guidance throughout the system life cycle.

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 directs FAA to review and update the framework to address known cybersecurity risks to the aviation system and short-term and long-term objectives for addressing these risks. The act also directs 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 directs FAA to develop an integrated cybersecurity testbed for air traffic control modernization technologies. It orders a National Academy of Sciences study to develop recommendations on how to increase the size, quality, and diversity of FAA's cybersecurity workforce.

P.L. 115-254 directs TSA to implement the framework for improving critical infrastructure cybersecurity developed by the National Institute of Standards and Technology to manage cybersecurity risks and conduct cybersecurity vulnerability assessments, including cybersecurity evaluations of the PreCheck program as well as transportation worker credentialing programs that contain data on individuals. The act also directs 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 directs 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.[36] 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 specific topic for congressional oversight during the 116th Congress.

[34] 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/.

[35] Government Accountability Office, *Air Traffic Control: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*, GAO-15-370, April 2015.

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

Transit and Passenger Rail Security[37]

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 balancing the desire for increased rail passenger security with 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); 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 some 76,000 buses carrying 19 million passengers each weekday in the United States. 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,[38] but Congress has 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 provider 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

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

[38] 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.

- engage the public and transit operators in the counterterrorism mission.[39]

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. However, GAO reported in 2017 that TSA had not identified or prioritized high-risk entities for the RMAST program to focus on.[40]

The surface transportation inspector program has been a focus of congressional interest. Issues of concern to Congress have included 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.[41] The number of surface inspectors declined from 404 in FY2011 to 222 (full-time equivalent positions) in FY2018. TSA attributed the decrease to efficiencies achieved through focusing efforts on the basis of risk.[42] 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.[43] 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.[44]

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.[45] 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

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

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

[41] 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.

[42] 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.

[43] 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.

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

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

information-sharing effort.[46] In a 2015 hearing, GAO testified that TSA had put processes in place to address these issues.[47]

DHS provides grants for security improvements for public transit, passenger rail, and occasionally other surface transportation modes under the Transit Security Grant Program. The vast majority of the funding goes to public transit providers. CRS estimates that, on an inflation-adjusted basis, funding for this program has declined 84% since 2009, when Congress allocated $150 million in the American Recovery and Reinvestment Act of 2009, in addition to routine appropriations (see **Table 1**).

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.[48] Despite this finding, Congress has not supported consolidation of the programs, though 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.

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

[47] 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.

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

Table 1. Congressional Funding for Transit Security Grants, FY2002-FY2018

Fiscal Year	Appropriation (millions of nominal dollars)	Appropriation (millions of 2018 dollars)
2002	$63[a]	$86
2003	65	87
2004	50	65
2005	108	137
2006	131	161
2007	251	301
2008	356	413
2009	498[b]	575
2010	253	288
2011	200	223
2012	88[c]	96
2013	84	90
2014	90	95
2015	87	92
2016	87	91
2017	88	90
2018	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; FY2012-2018: 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 2018 dollars using the Total Non-defense column from Table 10: Gross Domestic Product and Deflators Used in the Historical Tables: 1940-2023, published in the Historical Tables volume of the Budget of the United States Government, Fiscal Year 2019 (https://www.whitehouse.gov/omb/historical-tables/).

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.

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.

Port and Maritime Security[49]

The bulk of U.S. overseas trade is carried by ships, and thus the economic consequences 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 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. Customs 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 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.

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

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).

Two aspects of maritime security that have drawn attention recently are cybersecurity and the use of drones for coastal surveillance. 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. 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. 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.[50] The Coast Guard has added cybersecurity training to the requirements for mariner licensing and for port security officer qualifications.

Greater use of unmanned aircraft systems potentially offers significant efficiencies in performing various Coast Guard missions, including coastal surveillance. Congress has provided funding for the use of drones aboard national security cutters.[51] The Coast Guard has tested both hand-held drones and larger drone aircraft to extend the surveillance range of its patrol vessels. Since 2015, the Coast Guard has been testing UASs in the Arctic for missions such as surveying ice conditions, marine environmental monitoring, marine safety, and search and rescue.[52] The unmanned aircraft being tested each summer can be launched from land or a Coast Guard cutter.[53] The Coast Guard Authorization Act of 2018 (P.L. 115-282, §812) requests a study by the National Academy of Sciences as to how drones could be used to enhance the Coast Guard's maritime domain awareness. The act also allows the Coast Guard to lease but not design its own large UASs if funding is provided for design and construction of Offshore Patrol Cutters (§304).[54]

[50] Coast Guard, Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities, July 12, 2017.

[51] H.Rept. 114-215, DHS Appropriations Bill, 2016; p. 59.

[52] 80 *Federal Register* 18431, April 6, 2015.

[53] Coast Guard Compass, "Research, Development, Test and Evaluation Spotlight: Arctic Technology Evaluation 2018," September 11, 2018; http://coastguard.dodlive.mil/2018/09/research-development-test-and-evaluation-spotlight-arctic-technology-evaluation-2018/.

[54] Similar language was enacted in the National Defense Authorization Act for FY2017 (P.L. 114-328, §899).

Author Information

Bart Elias
Specialist in Aviation Policy

David Randall Peterman
Analyst in Transportation Policy

John Frittelli
Specialist in Transportation Policy

Disclaimer