

Transportation Security: Issues for the 115th Congress

(name redacted)

Specialist in Aviation Policy

(name redacted)

Analyst in Transportation Policy

(name redacted)

Specialist in Transportation Policy

January 5, 2017

Congressional Research Service

7-....

www.crs.gov

RL33512

Summary

The nation's air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them highly vulnerable to terrorist attack. While hardening the transportation sector from terrorist attack is difficult, measures can be taken to deter terrorists. The dilemma facing Congress is how best to construct and finance a system of deterrence, protection, and response that effectively reduces the possibility and consequences of another terrorist attack without unduly interfering with travel, commerce, and civil liberties.

Aviation security has been a major focus of transportation security policy since the terrorist attacks of September 11, 2001. In the aftermath of these 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 a federalized workforce of security screeners to inspect airline passengers and their baggage. The FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) included a number of aviation security provisions designed to expand the PreCheck program to expedite screening for known travelers, enhance background checks of airport workers and strengthen airport access controls, and improve passenger checkpoint efficiency and operational performance.

Until recently, TSA applied relatively uniform methods to screen airline passengers, focusing primarily on advances in screening technology to improve security and efficiency. TSA has recently shifted away from this approach, which assumes a uniform level of risk among all airline travelers, to risk-based screening approaches that focus more intensely on passengers thought to pose elevated security risks. Despite the extensive focus on aviation security over the past 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 airport workers with access to aircraft and sensitive areas;
- exploiting available intelligence information and watchlists to identify individuals who pose potential threats to civil aviation;
- effectively responding to security threats at airports and 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.

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 and the slow rate at which transit and rail security grants have been expended.

Existing law mandates the scanning of all U.S.-bound maritime containers with non-intrusive inspection equipment at overseas ports of loading by July 2012. This deadline was not met, and DHS is opposed to that strategy in favor of a risk-based, layered approach to security screening. Implementation of the Transportation Worker Identification Credential (TWIC) for port and maritime workers also appears to be experiencing continuing difficulties.

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.....	6
Perimeter Security, Access Controls, and Worker Vetting	7
Explosives Screening Technology and Canines.....	8
Event Response in the Non-sterile Area.....	8
Security Response to Incidents at Screening Checkpoints.....	9
Foreign Last Point of Departure Airports.....	9
Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft	10
Security Issues Regarding the Operation of Unmanned Aircraft	11
Aviation Cybersecurity.....	13
Transit and Passenger Rail Security	14
Port and Maritime Security Issues.....	18
Container Scanning Requirement.....	18
Transportation Worker Identification Credential (TWIC).....	19
Maritime Cybersecurity	20

Tables

Table 1. Congressional Funding for Transit Security Grants, FY2002-FY2016.....	17
--	----

Contacts

Author Contact Information	21
----------------------------------	----

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 construct 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 fire 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 from an attack, without imposing unduly burdensome requirements.

Aviation Security¹

Following the 9/11 terrorist attacks, Congress took swift action to create the Transportation Security Administration (TSA), federalizing all airline passenger and baggage screening functions and deploying significantly increased numbers of armed air marshals on commercial passenger flights. To this day, the federalization of airport screening remains controversial. For example, Representative Bill Shuster, chairman of the House Transportation and Infrastructure Committee, said in 2015 that, in hindsight, the decision to create TSA as a federal agency functionally responsible for passenger and baggage screening was a “big mistake,” and that frontline screening responsibilities should have been left in the hands of private security companies.² While airports have the option of opting out of federal screening, alternative private screening under TSA contracts has been limited to 21 airports out of approximately 450 commercial passenger airports where passenger screening is required.³ Congress has sought to ensure that optional private

¹ This section was prepared by (name redacted), Specialist in Aviation Policy.

² Keith Laing, “GOP Chairman: TSA was a ‘big mistake,’” *The Hill*, March 18, 2015, <http://thehill.com/policy/transportation/236130-gop-rep-creating-tsa-was-a-mistake>.

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

screening remains available for those airports that want to pursue this option, but 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;
- exploiting available intelligence information and watchlists to identify individuals who pose potential threats to civil aviation;
- effectively responding to security threats at airports and 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.

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 and domestic cargo carried aboard passenger aircraft meets 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 the October 2010 cargo aircraft bomb plot that originated in Yemen, to assess shipments for explosives threats or other terrorism-related activities.

Given the focus on the threats to aviation posed by explosives, a significant focus of TSA acquisition efforts has been on explosives screening technologies. However, in 2014, Congress found that TSA had failed to meet key performance requirements set for explosives detection and had not consistently implemented Department of Homeland Security (DHS) policy and best

practices for procurement.⁴ The Transportation Security Acquisition Reform Act (P.L. 113-245) addressed these concerns by requiring a five-year technology investment plan, and increased accountability for acquisitions through 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, as well as improvements in setting and attaining goals for small-business contracting opportunities.

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,⁵ has 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 (WBI) screening 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.⁶ 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.⁷ 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 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 to evaluate the effectiveness of AIT and ATR.⁸ In testimony, DHS Inspector General John Roth revealed that the covert testing consistently found failures in technology and procedures coupled with human error that allowed prohibited items to pass into secure areas.⁹

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

⁴ See P.L. 113-245.

⁵ Andrew Roth, "Russia: Terrorist Attack Brought Down Jetliner over Sinai," *Washington Post*, November 18, 2015, p. A8.

⁶ National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, New York, NY: W. W. Norton & Co., 2004.

⁷ See, e.g., American Civil Liberties Union. ACLU Backgrounder on Body Scanners and "Virtual Strip Searches," New York, NY, January 8, 2010.

⁸ Department of Homeland Security, Office of Inspector General, *DHS OIG Highlights: Covert Testing of the Transportation Security Administration's Passenger Screening Technologies and Processes at Airport Security Checkpoints*, OIG-15-150, September 22, 2015.

⁹ 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.

prohibit the use of WBI technology 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 FY2016, TSA deployed about 750 AIT units, roughly 86% of its projected full operating capability of 870 units. Full operating capability, once achieved, will still leave many smaller airports without 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, has not been rolled out at many smaller airports: currently, the program's incentive of expedited screening is offered at less than half of all commercial passenger airports.

In addition to continued deployment and utilization of AIT, the FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) directed TSA to task the Aviation Security Advisory Committee, composed of industry experts on airport and airline security matters, to develop recommendations for more efficient and effective passenger screening. It also directed TSA to initiate a pilot program at three to six large airports to examine passenger checkpoint reconfigurations that increase efficiencies and reduce vulnerabilities, and a separate pilot program at three airports to develop and test next-generation screening system prototypes designed to expedite passenger handling.

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 TSA's latest version of a trusted traveler program that has been modeled after CBP programs such as Global Entry, SENTRI, and NEXUS. Under the PreCheck 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 2016, PreCheck expedited screening lanes were available at more than 180 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. About 10 million individuals have enrolled in either PreCheck or other DHS trusted traveler programs, like Global Entry, that allow access to expedited screening lanes, but TSA would like to boost this number to 25 million.¹⁰

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

¹⁰ Kelly Yamanouchi, "Haven't Joined TSA PreCheck Yet? You're Not Alone," *Atlanta Journal Constitution*, June 17, 2016, <http://airport.blog.ajc.com/2016/06/14/havent-joined-tsa-precheck-yet-youre-not-alone/>.

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.¹¹

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.¹²

TSA phased out the managed inclusion program in the fall of 2015. Since September 2015, TSA behavior detection officers (BDOs) and explosives trace detection personnel no longer direct passengers not enrolled in PreCheck to expedited screening lanes. Passenger evaluations by canine explosives detection teams continue at some airports, but TSA is moving toward offering expedited screening only to PreCheck program enrollees.¹³ Questions remain regarding whether PreCheck is fully effective in directing security resources to unknown or elevated-risk travelers. Nonetheless, it has improved screening efficiency, resulting in cost savings for TSA. TSA estimates annual savings in screener workforce costs totaling \$110 million as a result of PreCheck and other risk-based initiatives.¹⁴

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.¹⁵ In July 2012, TSA expanded the program to include flight attendants.¹⁶

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 BDOs 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.¹⁷

¹¹ 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>.

¹² 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.

¹³ “TSA Explains Confusion over PreCheck Policies,” *TravelSkills*, September 23, 2015, <http://travelskills.com/2015/09/23/tsa-explains-confusion-over-precheck-policies/>.

¹⁴ Department of Homeland Security, Transportation Security Administration, Fiscal Year 2016 Congressional Justification, Aviation Security.

¹⁵ See <http://www.knowncrewmember.org/Pages/Home.aspx>.

¹⁶ 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>.

¹⁷ 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, (continued...)

P.L. 114-190 included language to expand capabilities of the TSA PreCheck program by involving private-sector entities in marketing PreCheck and enrolling applicants. The law mandates that PreCheck lanes be open and available during peak and high-volume travel times.

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 modified security directives to require airlines to check passenger names against the no-fly list within 2 hours of being electronically notified of an urgent update, instead of allowing 24 hours to recheck the list. The event also accelerated the transfer of watchlist checks from the airlines to TSA 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 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

Central issues surrounding the use of terrorist watchlists in the aviation domain that may be considered during the 115th 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 of Iraq and Syria (ISIS).²¹

(...continued)

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.

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 (name redacted) and (name redacted), available upon request.

²¹ For further details see CRS Report R44678, *The Terrorist Screening Database and Preventing Terrorist Travel*, by (continued...)

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 employees to look for proper identification and 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 offenses, 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.²²

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 services to identify disqualifying criminal offenses.

Language in P.L. 114-190 also directs TSA to conduct enhanced physical inspections of airport workers at SIDA access points and in SIDA areas. The inspections are to be random and

(...continued)

(name redacted), (name redacted), and (name redacted) CRS Report R43730, *Terrorist Databases and the No Fly List: Procedural Due Process and Other Legal Issues*, by (name redacted)

²² See <https://www.tsc-csc.com>.

unpredictable as well as data-driven and operationally dynamic. The law also directs TSA and the Department of Homeland Security Office of Inspector General to increase covert testing of access controls.

Explosives Screening Technology and Canines

Explosives screening technologies at passenger screening checkpoints primarily consist of whole body imaging systems known as Advanced Imaging Technology (AIT); advanced technology X-ray imagers for carry-on items; and explosives trace detection (ETD) systems used to test swab samples collected from individuals or carry-on items for explosives residue. In its FY2017 budget request, TSA indicated that it intends to procure AIT and ETD systems in small numbers, while it intends to acquire more than 300 advanced technology X-ray imagers for carry-on items, upgraded with multi-view capabilities or automated explosives detection capabilities.

For checked baggage screening, TSA utilizes explosives detection system (EDS) and ETD 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) EDS systems, depending on airport needs and configurations. The use of explosives detection technology was mandated by the Aviation and Transportation Security Act (ATSA; P.L. 107-71) more than a decade ago. Consequently, present TSA checked-baggage explosives detection technology acquisition is primarily focused on replacing systems that have reached the end of their service lives. 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 320 TSA teams and 675 state and local law enforcement teams trained by TSA under partnership agreements. More than 180 of the TSA teams are dedicated to passenger screening at about 40 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 included language authorizing 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 along with other resources and technologies to minimize passenger wait times and maximize security effectiveness of checkpoint operations.

Event Response in the Non-sterile Area

Incident response at airports is primarily the responsibility of the airport operator and state or local law enforcement agencies, with TSA acting as a regulator in approving response plans as part of an airport's comprehensive security program. Federal law enforcement may also be involved in developing and reviewing these 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.

The Brussels and Istanbul airport bombings increased concern over response to security incidents in non-sterile areas of airports prior to passenger screening checkpoints. Language in P.L. 114-190 establishes requirements for DHS to develop training exercises to enhance law enforcement

and first responder preparedness for active shooter and mass casualty events at airports, mass transit systems, and other public locations.

Security Response to Incidents 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, including enhanced active shooter incident training for screeners; better coordination and dissemination of information regarding incidents; expansion and routine testing of alert notification capabilities; and expanded law enforcement presence at checkpoints during peak times. TSA 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. Such plans must include details on evacuation, unified incident command, testing and evaluation of communications, time frames for law enforcement response, and joint exercises and training at airports. Additionally, the act requires TSA 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. Law enforcement response to incidents at passenger screening checkpoints allows for flexibility in the deployment of law enforcement support. While some airports station law enforcement officers at dedicated posts at or near passenger screening checkpoints, other airports allow officers to patrol other areas of the airport so long as a minimum response time to incidents at passenger screening checkpoints is maintained. TSA provides funding for law enforcement support at screening checkpoints through agreements that partially reimburse for law enforcement hours.

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.

TSA 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.

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

²³ See 49 C.F.R. Part 1546.

connecting flights or leave the airport directly, rather than being routed to customs and immigration processing facilities. 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 airport of entry, which has been the practice. So far, four preclearance airports have been approved for checked baggage preclearance operations, and TSA has indicated that five more locations are expected to be approved soon.²⁴

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.

Mitigating the Threat of Shoulder-Fired Missiles to Civilian Aircraft

The threat to civilian aircraft posed by shoulder-fired missiles or other standoff weapons capable of downing an airliner remains a vexing concern for aviation security specialists and policymakers. The State Department has estimated that, since the 1970s, over 40 civilian aircraft have been hit by shoulder-fired missiles, causing 25 crashes and more than 600 deaths. Most of these incidents involved small aircraft operated at low altitudes in areas of ongoing armed conflicts, although some larger jets have also been destroyed. On July 17, 2014, Malaysia Airlines Flight 17, a Boeing 777, was shot down over eastern Ukraine by a much larger surface-to-air missile.

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, the first such event outside of a conflict zone. In 2003, then Secretary of State Colin Powell remarked that there was “no threat more serious to aviation.”²⁵ Since then, Department of State and military initiatives seeking bilateral cooperation and voluntary reductions of man-portable air defense systems (MANPADS) stockpiles had reduced worldwide inventories by nearly 33,000 missiles.²⁶ Despite this progress, such weapons may still be in the hands of terrorist organizations. Conflicts in Libya and Syria have renewed concerns that large military stockpiles of these weapons may be proliferated to radical insurgent groups like Ansar al-Sharia in Libya, Al Qaeda in the Islamic Maghreb (AQIM), and the Islamic State in Iraq and Syria (ISIS).²⁷ This threat, combined with the limited capability to improve

²⁴ Department of Homeland Security, *Congressional Budget Justification, FY2017- Volume II, U.S. Immigration and Customs Enforcement, Transportation Security Administration, U.S. Coast Guard*.

²⁵ Katie Drummond, “Where Have All the MANPADS Gone?,” *Wired*, February 22, 2010.

²⁶ U.S. Department of State, *Addressing the Challenge of MANPADS Proliferation*, Remarks of Andrew J. Shapiro, Assistant Secretary, Bureau of Political-Military Affairs, Stimson Center, Washington, DC, February 2, 2012, <https://www.state.gov/t/pm/rls/rm/183097.htm>; Andrew J. Shapiro, Assistant Secretary, Bureau of Political-Military Affairs, U.S. Department of State, *Addressing the Challenge of MANPADS Proliferation*, Remarks, Stimson Center, Washington, DC, February 2, 2012, <http://www.state.gov/t/pm/rls/rm/183097.htm>.

²⁷ See Andrew J. Shapiro, Assistant Secretary, Bureau of Political-Military Affairs, U.S. Department of State, *Addressing the Challenge of MANPADS Proliferation*, Remarks, Stimson Center, Washington, DC, February 2, 2012, <http://www.state.gov/t/pm/rls/rm/183097.htm>; Thomas Gibbons-Neft, “Islamic State Might Have Taken Advanced MANPADS from Syrian Airfield,” *Washington Post*, August 24, 2014; Sharyl Attkisson, “Thousands of Libyan Missiles from Qaddafi Era Missing in Action,” *CBS News*, March 25, 2013, <http://www.cbsnews.com/news/thousands-of-libyan-missiles-from-qaddafi-era-missing-in-action/>.

security beyond airport perimeters and to modify flight paths, leaves civil aircraft vulnerable to missile attacks, particularly in and near conflict zones.

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 operational and live-fire testing along with Federal Aviation Administration (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. Although the units do not protect against the full range of potential weapons that pose a potential threat to civil airliners, they do appear to provide effective protection against what is likely the most menacing standoff threat: heat-seeking MANPADS. Nonetheless, 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. Policy discussions have focused mostly on whether to fund the acquisition of limited numbers of the units for use by the Civil Reserve Aviation Fleet, civilian airliners that can be called up to transport troops and supplies for the military. Other approaches to protecting aircraft, including ground-based missile countermeasures and escort planes or drones equipped with antimissile technology, have been considered on a more limited basis, but these options face operational challenges that may limit their effectiveness.

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 of flight paths to potential MANPADS attacks face significant challenges because of limited resources and large geographic areas where aircraft are vulnerable to attack. Any terrorist attempts to exploit those vulnerabilities could quickly escalate the threat of shoulder-fired missiles to a major national security priority.

Security Issues Regarding the Operation of Unmanned Aircraft

Provisions in the FAA Modernization and Reform Act of 2012 (P.L. 112-95) required that FAA take steps by the end of FY2015 to accommodate routine operation of unmanned aircraft systems (UASs, widely referred to as “drones”) in domestic airspace. Although this deadline was not met, FAA has taken a number of steps to accommodate flights by small UASs for both recreational and commercial purposes.

The operation of civilian UASs in domestic airspace 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.

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. The incident heightened concern about potential terrorist attacks using unmanned aircraft. Widely publicized drone incidents, including 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; and a series of unidentified drone flights over landmarks and sensitive locations in Paris, France, in 2015, have raised additional concerns about 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. The payload capacities of small unmanned aircraft would limit the damage a terrorist attack using conventional explosives could inflict, but drone attacks using chemical, biological, or radiological weapons could be more serious.

An FAA proposal for regulating small unmanned aircraft used for commercial purposes would require TSA to carry out threat assessments of certificated operators as it does for civilian pilots.²⁸ However, this requirement would 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,²⁹ it is not clear that law enforcement agencies have sufficient training or technical capacity to respond to this emerging threat.³⁰

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.³¹

TSA has broad statutory authority over aviation security issues; it has not formally addressed the potential security concerns arising from unmanned aircraft operations in domestic airspace.

While unmanned aircraft may pose security risks, they are also a potential asset for homeland security operations, particularly for CBP border surveillance. CBP currently employs a fleet of 10 modified Predator UASs, and has plans to acquire another 14, to augment its border-patrol capabilities. Operating within specially designated airspace, these unarmed UASs patrol the northern and southern land borders and the Gulf of Mexico to detect potential border violations and monitor suspected drug trafficking, with UAS operators cuing manned responses when appropriate. State and local governments have expressed interest in operating UASs for missions as diverse as traffic patrol, surveillance, and event security. A small but growing number of state and local agencies have acquired drones, some through federal grant programs, and have been issued special authorizations by FAA to fly them. However, many federal, state, and local agencies involved in law enforcement and homeland security appear to be awaiting more specific guidance from FAA regarding the routine operation of public-use unmanned aircraft in domestic airspace.

The introduction of drones into domestic surveillance operations presents a host of novel legal issues related to an individual’s fundamental privacy interest protected under the Fourth Amendment.³² To determine if certain government conduct constitutes a search or seizure under that amendment, courts apply an array of tests (depending on the nature of the government action), including the widely used reasonable expectation of privacy test. When applying these

²⁸ Federal Aviation Administration, “Operation and Certification of Small Unmanned Aircraft Systems; Proposed Rule,” 80 *Federal Register* 9544-9590, February 23, 2015.

²⁹ 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.

³⁰ 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.

³¹ 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.

³² See CRS Report R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, by (name redacted).

tests to drone surveillance, a reviewing court will likely examine the location of the search, the sophistication of the technology used, and society's conception of privacy. For instance, while individuals are accorded substantial protections against warrantless government intrusions into their homes,³³ the Fourth Amendment offers fewer restrictions upon government surveillance occurring in public places,³⁴ and even fewer at national borders.³⁵ Likewise, drone surveillance conducted with relatively unsophisticated technology might be subjected to a lower level of judicial scrutiny than investigations conducted with advanced technologies such as thermal imaging or facial recognition. Several measures introduced in Congress would require government agents to obtain warrants before using drones for domestic surveillance, but would create exceptions for patrols of the national borders used to prevent or deter illegal entry and for investigations of credible terrorist threats.³⁶

Language in P.L. 114-190 directs 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 directs FAA to develop an air traffic management system for small UASs that, in addition to addressing safety concerns, could include measures to detect and deter security threats posed by UASs.

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 the Federal Aviation Administration (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 2012.³⁷ 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.³⁸

³³ See the U.S. Supreme Court decision in *Kyllo v. United States*, 533 U.S. 27 (2001).

³⁴ See *California v. Ciraolo*, 476 U.S. 207, 213 (“[W]hat a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection”) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)).

³⁵ See, e.g., *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004) (“The Government’s interest in preventing the entry of unwanted persons and effects is at its zenith at the international border”).

³⁶ See, e.g., H.R. 1229, H.R. 1385, S. 635.

³⁷ 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.

³⁸ 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/>.

In recognition of those threats, FAA has developed a software assurance policy for all FAA-owned and FAA-controlled information systems.³⁹ However, according to an April 2015 GAO report, while FAA has taken steps to protect air traffic control systems from cyberthreats, it lacks a formal cybersecurity threat model. Moreover, GAO found that FAA faces continuing challenges in mitigating cyberthreats, particularly as it transforms air traffic control systems under its NextGen modernization initiative.⁴⁰

For systems onboard aircraft, FAA requires security and integrity to be addressed in the airworthiness certification process. In other words, under the existing regulatory framework for aircraft certification, cybersecurity risks must be satisfactorily mitigated. Large commercial aircraft and aviation systems manufacturers now typically collaborate with software security companies in order to attain high levels of assurance for software embedded in avionics equipment, but these approaches are still evolving. 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 and advised airlines to look out for individuals trying to tap into aircraft electronics and for any evidence of tampering or network intrusions.⁴¹

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.⁴² 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 mandates development of a comprehensive strategic framework for reducing cybersecurity risks to the national airspace system, civilian aviation, and FAA information systems. The framework is to address cybersecurity risks associated with airspace modernization, aircraft automation, and in-flight entertainment systems. The act also directs FAA to assess the cost and schedule for developing and maintaining an agency-wide cybersecurity threat model as recommended by GAO, and produce a standards plan to implement security guidance for FAA data and information systems.

Transit and Passenger Rail Security⁴³

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

³⁹ Federal Aviation Administration, "Order 1370.109: National Policy, Software Assurance Policy," effective October 23, 2009.

⁴⁰ 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.

⁴¹ 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/>.

⁴² 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.

⁴³ This section was prepared by (name redacted), Analyst in Transportation Policy.

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, with the potential costs and damages of an attack, and with 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, as well as the consequences, of an attack. 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 role is one of oversight, coordination, intelligence sharing, training, and assistance, though it does provide 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.”

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), passed by Congress on July 27, 2007, included provisions on passenger rail and transit security and authorized \$3.5 billion for FY2008-FY2011 for grants for public transportation security. The act required public transportation agencies and railroads considered to be high-risk targets by DHS to have security plans approved by DHS (§1405 and §1512). Other provisions required DHS to conduct a name-based security background check and an immigration status check on all public transportation and railroad frontline employees (§1414 and §1522), and gave DHS the authority to regulate rail and transit employee security training standards (§1408 and §1517).

In 2010 TSA completed a national threat assessment for transit and passenger rail, and in 2011 completed an updated transportation systems sector-specific plan, which established goals and objectives for a secure transportation system. The three primary objectives for reducing risk in transit are

- 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.⁴⁴

⁴⁴ Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2016 Congressional [Budget] Justification*, p. 11.

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 (I-STEP).

The House Committee on Homeland Security's Subcommittee on Transportation Security held a hearing in May 2012 to examine the surface transportation security inspector program. The number of inspectors had increased from 175 in FY2008 to 404 in FY2011 (full-time equivalents). Issues considered at the hearing included the lack of surface transportation expertise among the inspectors, many of whom were promoted from screening passengers at airports; the administrative challenge of having the surface inspectors managed by federal security directors who are located at airports and who themselves typically have no surface transportation experience; and the security value of the tasks performed by surface inspectors.⁴⁵ The number of surface inspectors decreased to 260 (full-time equivalent positions) in FY2016, in part reflecting a reduction in the number of VIPR surface inspectors and in part reflecting efficiencies achieved through focusing efforts on the basis of risk.⁴⁶

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.⁴⁷ 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.⁴⁸ In a 2015 hearing, GAO testified that TSA has put processes in place to address these issues.⁴⁹

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, in addition to routine appropriations (see **Table 1**).

⁴⁵ 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>.

⁴⁶ 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.

⁴⁷ Government Accountability Office, *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*, GAO-13-20, December 19, 2012.

⁴⁸ Government Accountability Office, *Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts*, GAO-14-506, June 24, 2014.

⁴⁹ 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.

Table I. Congressional Funding for Transit Security Grants, FY2002-FY2016

Fiscal Year	Appropriation (millions of nominal dollars)	Appropriation (millions of 2015 dollars)
2002	\$63 ^a	82
2003	65	83
2004	50	62
2005	108	131
2006	131	154
2007	251	287
2008	356	394
2009	498 ^b	549
2010	253	275
2011	200	213
2012	88 ^c	92
2013	84	86
2014	90	91
2015	87 ^d	87
2016	87 ^d	87

Source: FY2002: Department of Defense FY2002 Appropriations Act, P.L. 107-117; FY2003: FY2003 Emergency Wartime Supplemental Appropriations Act, P.L. 108-111; 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 I; FY2012-2014: DHS, Transit Security Grant Program annual funding opportunity announcements; FY2015: P.L. 114-4; FY2016: P.L. 114-113.

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 2015 dollars using the Total Non-defense column from Table 10: Gross Domestic Product and Deflators Used in the Historical Tables: 1940-2020, published in the Historical Tables volume of the Budget of the United States Government, Fiscal Year 2016 (<http://www.whitehouse.gov/omb/budget/Historicals>).

- 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.
- d. Estimated by CRS; Congress provided \$100 million for Public Transportation, Amtrak, and Over-the-Road Bus Security grants, and specified that no less than \$10 million was for Amtrak and no less than \$3 million was for bus grants (P.L. 114-4 and P.L. 114-113).

In a February 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.⁵⁰ The Obama Administration has repeatedly proposed consolidating several of these programs in annual budget requests. This proposal has not been supported by Congress in the appropriations process to date, though appropriators have expressed concerns that grant

⁵⁰ United States Governmental Accountability Office, *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, GAO-12-303, February 2012.

programs have not focused on areas of highest risk and that significant amounts of previously appropriated funds have not yet been awarded to recipients.

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 Issues⁵¹

The bulk of U.S. overseas trade is carried by ships and thus the economic consequences of a maritime terrorist attack could be significant. A key challenge for U.S. policymakers is prioritizing maritime security activities among a virtually unlimited number of potential attack scenarios. One priority is preventing the smuggling of a weapon of mass destruction in a shipping container. A less complicated attack scenario is ramming a passenger vessel with a bomb-laden speedboat. There are far more potential attack scenarios than likely ones, and far more than could be meaningfully addressed with limited counterterrorism resources. Not all terrorist groups have familiarity with the maritime environment. Two port security initiatives the 115th Congress may continue to examine are the 100% container scanning requirement and the effectiveness of a port worker security card system. Cybersecurity is an emerging concern.

Container Scanning Requirement

Section 1701 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires that all imported marine containers be scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign loading port by July 1, 2012, unless DHS can demonstrate it is not feasible, in which case the deadline can be extended by two years on a port-by-port basis. DHS has sought a blanket extension for all ports, citing numerous challenges to implementing the 100% scanning requirement at overseas ports.⁵² In a letter requesting renewal of the two-year extension, DHS Secretary Jeh Johnson stated,⁵³

I have personally reviewed our current port security and DHS's short term and long term ability to comply with 100% scanning requirement. Following this review, I must report, in all candor, that DHS's ability to fully comply with this unfunded mandate of 100% scanning, even in the long term, is highly improbable, hugely expensive, and in our judgment, not the best use of taxpayer resources to meet this country's port security and homeland security needs.

In an October 2015 hearing, DHS officials reiterated their opposition to a 100% scanning strategy in favor of a risk-based and layered security strategy.⁵⁴ Major U.S. trading partners also oppose 100% scanning. The European Commission has determined that 100% scanning is the wrong approach, favoring a multilayered risk management approach to inspecting cargo.⁵⁵ CBP has

⁵¹ This section was prepared by (name redacted), Specialist in Transportation Policy.

⁵² Testimony of Janet Napolitano, Secretary of DHS, before the Committee on Commerce, Science, and Transportation, U.S. Senate, hearing "Transportation Security Challenges Post 9-11," December 2, 2009.

⁵³ Letter from DHS Secretary Jeh Johnson to Senator Carper, Chairman of the Senate Committee on Homeland Security and Governmental Affairs, May 5, 2014.

⁵⁴ House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, Hearing—*The Prevention of and Response to the Arrival of a Dirty Bomb at a U.S. Port*, October 27, 2015. In particular, see the oral and written testimonies of officials from CBP and the Domestic Nuclear Detection Office.

⁵⁵ European Commission Staff Working Paper, *Secure Trade and 100% Scanning of Containers*, February 2010, http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/sec_2010_131_en.pdf.

tested the feasibility of scanning all U.S.-bound containers at several overseas ports⁵⁶ and identified numerous operational, technical, logistical, financial, and diplomatic obstacles,⁵⁷ including opposition from host government officials.⁵⁸ In a July 2016 hearing, DHS officials restated their opposition to pursuing a 100% scanning strategy.⁵⁹ One-hundred-percent scanning conflicts with DHS's general approach to risk management, which seeks to focus scarce inspection resources on the highest-risk containers. By scanning a smaller number of containers, DHS may be able to devote additional resources to each individual scan. This consideration is important because reviewing the scans is labor-intensive, and scanning fewer containers may allow DHS to subject individual scans to greater scrutiny, and to maintain a lower threshold for opening containers with questionable scanning images.

If illicit cargo is estimated to be limited to less than 1% of incoming containers, as CBP believes to be the case, focusing enforcement on the likeliest containers may be the most effective enforcement strategy. This approach would emphasize risk-based scanning along with investment in CBP intelligence to improve targeting, and/or increase CBP personnel, which would allow ports to conduct a larger number of targeted special enforcement operations.

Transportation Worker Identification Credential (TWIC)

In January 2007, TSA and the Coast Guard issued a final rule implementing the Transportation Worker Identification Credential (TWIC) at U.S. ports.⁶⁰ Longshoremen, port truck drivers, railroad workers, merchant mariners, and other workers at a port must apply for a TWIC card to obtain unescorted access to secure areas of port facilities or vessels.⁶¹ The card was authorized under the Maritime Transportation Security Act of 2002 (MTSA; §102 of P.L. 107-295). As of October 2015, the population of TWIC holders was approximately 2.1 million.⁶² The card must be renewed every five years.

TSA conducts a security threat assessment of each worker before issuing a card. The security threat assessment uses the same procedures and standards established by TSA for truck drivers carrying hazardous materials, including examination of the applicant's criminal history, immigration status, and possible links to terrorist activity to determine whether a worker poses a security threat. A worker pays a fee of about \$130 that is intended to cover the cost of administering the cards. The card uses biometric technology for positive identification. Terminal operators were to deploy card readers at the gates to their facilities, so that a worker's fingerprint template would be scanned each time he or she entered the port area and matched to the data on the card.

⁵⁶ This test was conducted as per Section 231 of the SAFE Port Act (P.L. 109-347).

⁵⁷ CBP, "Report to Congress on Integrated Scanning System Pilots (Security and Accountability for Every Port Act of 2006, §231)," http://www.apl.com/security/documents/sfi_finalreport.pdf.

⁵⁸ Ibid., Appendix A.

⁵⁹ House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, Hearing—*An Examination of the Maritime Nuclear Smuggling Threat and Other Port Security and Smuggling Risks in the U.S.*, July 7, 2016.

⁶⁰ 72 *Federal Register*, 3492-3604, January 25, 2007. Codified at 49 C.F.R. §1572.

⁶¹ A TWIC does not entitle a card holder to enter a maritime facility. The facility owner has the authority and responsibility to determine if the person has a legitimate business purpose for entering its facility.

⁶² DHS, Office of Inspector General, "TWIC Background Checks are Not as Reliable as They Could Be," OIG-16-128, September 1, 2016, p. 2.

Finding a card reader that worked reliably in a harsh marine environment proved difficult. On August 23, 2016, the Coast Guard issued a final rule requiring that only the highest-risk maritime facilities—generally, those handling dangerous cargoes in bulk or passenger vessels with space for more than 1,000 passengers—install card readers. This effectively required about 525 of the roughly 3,200 maritime facilities regulated under MTSA to have card readers. Other facilities, including those handling containerized cargo, would continue to use the TWIC as a “flash pass,” but the biometric data on the card would not be used to positively identify the worker. Potential problems with this approach were highlighted by the February 2016 announcement that federal investigators uncovered a “document mill” producing fraudulent TWIC cards in Los Angeles.⁶³ The final rule becomes effective on August 23, 2018. Currently, the Coast Guard performs spot checks with hand-held biometric readers while conducting port security inspections.

GAO and Inspector General audits have been highly critical of how the TWIC has been implemented. A 2013 GAO audit found that the results of a pilot test of card readers should not be relied upon for developing regulations on card reader requirements because they were incomplete, inaccurate, and unreliable.⁶⁴ This audit was discussed at a hearing by the House Subcommittee on Government Operations on May 9, 2013,⁶⁵ and by the House Subcommittee on Border and Maritime Security on June 18, 2013.⁶⁶ Another 2013 GAO audit examined TSA’s Adjudication Center (which performs security threat assessments on TWIC applicants and other transportation workers), and recommended steps the agency could take to better measure the center’s performance.⁶⁷ A 2011 GAO audit found internal control weaknesses in the enrollment, background checking, and use of the TWIC card at ports, which were said to undermine the effectiveness of the credential in screening out unqualified individuals from obtaining access to port facilities.⁶⁸ Similarly, a 2016 Inspector General audit found that TSA appeared to be more concerned with customer service matters such as issuing the cards in a timely manner than with careful scrutiny of applicants.⁶⁹ It found that applicants believed to be providing fraudulent identification documents were nevertheless issued a TWIC.

The 114th Congress enacted the Essential Transportation Worker Identification Credential Assessment Act (P.L. 114-278), which requires TSA to improve its vetting process, including fraud detection. The law also requires DHS to commission an outside organization to conduct a comprehensive assessment of the benefits and costs of the TWIC card.

Maritime Cybersecurity

In June 2015, the Coast Guard released a document that identifies the agency’s plans for addressing cybersecurity in the maritime environment. Vessel and facility operators use

⁶³ IHS Fairplay Daily News, “Fake TWIC Cards Prompt U.S. Port Security Concerns,” February 10, 2016.

⁶⁴ U.S. Government Accountability Office, *Transportation Worker Identification Credential—Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed*, GAO-13-198, May 8, 2013.

⁶⁵ U.S. Congress, House Committee on Oversight and Government Reform, Subcommittee on Government Operations, *Federal Government Approaches to Issuing Biometric IDs*, 113th Cong., 1st sess., May 9, 2013.

⁶⁶ U.S. Congress, House Committee on Homeland Security, Subcommittee on Border and Maritime Security, *Threat, Risk and Vulnerability: the TWIC Program*, 113th Cong., 1st sess., June 18, 2013.

⁶⁷ U.S. Government Accountability Office, *Transportation Security: Action Needed to Strengthen TSA’s Security Threat Assessment Process*, GAO-13-629, July 19, 2013.

⁶⁸ U.S. Government Accountability Office, *Transportation Worker Identification Credential—Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, May 2011, GAO-11-657.

⁶⁹ DHS, Office of Inspector General, “TWIC Background Checks are Not as Reliable as They Could Be,” OIG-16-128, September 1, 2016.

potentially vulnerable technologies for navigation, communication, cargo handling, and other purposes. The strategy document states the Coast Guard will be developing guidance for vessels and ports to address vulnerabilities, and will incorporate cybersecurity into existing enforcement and compliance programs.⁷⁰ The strategy also states the Coast Guard will incorporate cybersecurity training in the requirements for mariner licensing and for port security officer qualifications. According to this document, the Coast Guard will modify an existing port risk assessment tool (MSRAM-Maritime Security Risk Assessment Model) to incorporate cyber risks. MSRAM is the primary tool used to assess risk to national infrastructure in the maritime domain, and is used extensively at the local, regional, and national levels, according to the Coast Guard.

In the 114th Congress, House-passed H.R. 3878 sought to promote cybersecurity risk information sharing among maritime stakeholders and provide industry with risk assessment tools. House-passed H.R. 5077 would have required DHS to report on U.S. maritime cyber threats and vulnerabilities (§604). The Senate did not act on either bill.

Author Contact Information

(name redacted)
Specialist in Aviation Policy
[redacted]@crs.loc.gov...

(name redacted)
Analyst in Transportation Policy
[redacted]@crs.loc.gov , 7-....

(name redacted)
Specialist in Transportation Policy
[redacted]@crs.loc.gov-....

⁷⁰ U.S. Coast Guard, “Cyber Strategy,” June 2015, pp. 32-33; <https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf>.

EveryCRSReport.com

The Congressional Research Service (CRS) is a federal legislative branch agency, housed inside the Library of Congress, charged with providing the United States Congress non-partisan advice on issues that may come before Congress.

EveryCRSReport.com republishes CRS reports that are available to all Congressional staff. The reports are not classified, and Members of Congress routinely make individual reports available to the public.

Prior to our republication, we redacted names, phone numbers and email addresses of analysts who produced the reports. We also added this page to the report. We have not intentionally made any other changes to any report published on EveryCRSReport.com.

CRS reports, as a work of the United States government, are not subject to copyright protection in the United States. Any CRS report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS report may include copyrighted images or material from a third party, you may need to obtain permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

Information in a CRS report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to members of Congress in connection with CRS' institutional role.

EveryCRSReport.com is not a government website and is not affiliated with CRS. We do not claim copyright on any CRS report we have republished.