Transportation Security: Issues for the 113th Congress

David Randall Peterman
Analyst in Transportation Policy

Bart Elias
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

January 11, 2013

Congressional Research Service
7-5700
www.crs.gov
RL33512

CRS Report for Congress
Prepared for Members and Committees of Congress

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 following 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. Despite extensive focus on aviation security over the past decade, a number of challenges remain, including

- effectively screening passengers, baggage, and cargo for explosive 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;
- 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.

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 that may continue in the 113th 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, in part because foreign countries object to the costs of this screening and are dubious of the benefits. The usefulness of this mandate, as well as continuing difficulties in fully implementing the Transportation Worker Identification Credential (TWIC) for port and maritime workers, continues to be of interest to Congress.

Contents

Tables

Contacts

Introduction

The nation's air, land, and marine transportation systems are designed for accessibility and efficiency, two characteristics that make them vulnerable to attack. The difficulty and cost of protecting the transportation sector from attack raises a core question for policymakers: how much effort and resources to put toward protecting potential targets versus pursuing and fighting terrorists. While hardening the transportation sector from 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 another terrorist attack 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 speed boat 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 Security[1]

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 large numbers of armed air marshals on commercial passenger flights. Despite extensive focus on aviation security over the past decade, a number of challenges remain, including

- effectively screening passengers, baggage, and cargo for explosive 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;

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

- 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. While TSA has met the requirement for cargo screening domestically, largely through implementation of its Certified Cargo Screening Program to oversee screening at off-airport shipping and consolidation facilities combined with supply chain security measures, additional work is needed to implement similar measures for U.S.-bound international flights.[2] Although TSA has yet to fully implement 100% screening of cargo placed on international flights, recent attention has particularly focused on improving explosives screening of passengers in response to continued threats.

On December 25, 2009, a passenger attempted to detonate an explosive device concealed in his underwear aboard Northwest Airlines flight 253 during its approach to Detroit, MI. Al Qaeda in the Arabian Peninsula claimed responsibility. Al Qaeda and its various factions have maintained a particular interest in attacking U.S.-bound airliners. Since 9/11, Al Qaeda has also been linked to the Richard Reid shoe bombing incident aboard American Airlines flight 63 en route from Paris to Miami on December 22, 2001, a plot to bomb several trans-Atlantic flights departing the United Kingdom for North America in 2006, and the October 2010 plot to detonate explosives concealed in air cargo shipments bound for the United States. In response to the Northwest Airlines flight 253 incident, 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 responds to the 9/11 commission recommendation to improve the detection of explosives on passengers.[3]

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 if used for primary screening.[4] The screening of children, the elderly, and individuals with medical conditions and disabilities has been particularly contentious. Recent modifications to pat-down screening procedures, involving

[2] See CRS Report R41515, *Screening and Securing Air Cargo: Background and Issues for Congress*, by Bart Elias.

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

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

more detailed inspection of private areas, have also raised privacy concerns.[5] To allay privacy concerns, TSA currently requires remote screening of images outside of public view and forbids recording or storage of AIT images. It has also begun implementing automated threat detection capabilities using automated targeting recognition (ATR) software that will eliminate the need for TSA screeners to view AIT-generated images.

Other concerns about AIT include the amount of time it takes to screen passengers and the potential medical risks posed by backscatter X-ray systems, despite assurances that the radiation doses from screening are comparatively small. Some have advocated for risk-based use of AIT, in coordination with the risk-based approaches to passenger screening discussed below. Past legislative proposals have specifically sought to prohibit the use of WBI technology for primary screening (see, e.g., H.R. 2200, 111th Congress), while more recent legislative proposals have sought to accelerate the deployment of ATR software and the phase-out of AIT systems not capable of automated threat detection (see H.R. 3011, 112th Congress).[6]

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. Initiatives include a new trusted traveler trial program called PreCheck, modified screening procedures for children 12 and under, and a trial program for expedited screening of known flight crew and cabin crew members. Trial programs are also under way for modified screening of elderly passengers similar to those procedures put in place for children. These various trial programs may allow for improved screening efficiencies and potential cost savings.

A cornerstone of TSA's risk-based initiatives is the PreCheck program. PreCheck is TSA's latest version of a trusted traveler program that has been modeled after similar Customs and Border Protection (CBP) programs including Global Entry, SENTRI, and NEXUS. It is currently available on a trial basis to members of those programs, frequent flyer program members of five major airlines, and, in some cases, to military service members, at a limited number of airports. Children 12 and younger traveling with PreCheck participants are also permitted to travel through the expedited screening lanes. A similar test program, called the Registered Traveler program, which involved private vendors that issued and scanned participants' biometric credentials, was scrapped by TSA in 2009 because it failed to show a demonstrable security benefit. Questions remain regarding whether PreCheck will be effective in directing security resources to unknown or elevated-risk travelers while expediting the screening of program participants.

One concern raised over PreCheck is the public dissemination of instructions, posted on Internet sites, detailing how to decipher boarding passes to determine whether a passenger has been selected for expedited screening. The lack of encryption could be exploited to attempt to avoid detection of threat items by more extensive security measures. Other concerns raised over the program include the lack of biometric identity authentication and the lack of detailed background

[5] Donna Goodison, "Passengers Shocked by New Touchy-Feely TSA Screening," *Boston Herald,* August 24, 2010.

[6] For further reading see CRS Report R42750, *Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening*, by Bart Elias.

checks, particularly for participants who qualify for PreCheck solely on the basis of their frequent flyer status.[7]

In addition to passenger screening, TSA, in coordination with participating airlines and labor organizations representing airline pilots, has initiated a known crewmember program to expedite security screening of airline flight crews.[8] In July 2012, TSA expanded the program to include flight attendants.[9]

TSA has also developed a passenger behavior detection program to identify potential threats based on observed behavioral characteristics. In addition to employing observational techniques, TSA behavior detection officers are field testing more extensive passenger interviews based on methods employed at Israeli airports.[10] Questions remain regarding the effectiveness of the behavioral detection program, and privacy advocates have cautioned that it could devolve into racial or ethnic profiling of passengers despite concerted efforts to focus solely on behaviors rather than individual passenger traits or characteristics. While TSA has proposed to increase the numbers of behavior detection officers by 72 to 3,131 in FY2013, the House Appropriations Committee did not support this increase, citing TSA's lack of clear evidence that behavior detection improves aviation security. The committee has called for a formal cost-benefit analysis of the program, along with a robust risk-based strategy for deploying behavior detection officers.[11]

The Use of Terrorist Watchlists in the Aviation Domain

The failed bombing attempt of Northwest Airlines flight 253 on December 25, 2009, also raised policy questions regarding the effective use of terrorist watchlists and intelligence information to identify individuals who may pose a threat to aviation. Specific failings to include the bomber on either the no-fly or selectee list, despite intelligence information suggesting that he posed a security threat, prompted reviews of the intelligence analysis and terrorist watchlisting processes. Adding to these concerns, on the evening of May 3, 2010, Faisal Shazad, a suspect in an attempted car bombing in New York's Times Square, was permitted to board an Emirates Airline flight to Dubai at the John F. Kennedy International airport, even though his name had been added to the no-fly list earlier in the day. He was subsequently identified, removed from the aircraft, and arrested after the airline forwarded the final passenger manifest to CBP's National Targeting Center just prior to departure.[12] Subsequently, TSA modified security directives to require airlines to check passenger names against the no-fly list within two 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.

---

[7] Robert Poole, "Problems and Progress with PreCheck," *Airport Policy and Security News #84*, November 5, 2012, The Reason Foundation, Los Angeles, http://reason.org/news/show/airport-policy-and-security-news-84.

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

[9] 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.

[10] Katie Johnston, "A Question for You," *Boston Globe*, August 3, 2011.

[11] H.Rept. 112-492, pp. 65-66.

[12] Scott Shane, "Lapses Allowed Suspect to Board Plane," *New York Times*, May 4, 2010.

By the end of November 2010, the Department of Homeland Security (DHS) announced that 100% of passengers flying to or from U.S. airports are being vetted using the Secure Flight system.[13] Secure Flight continues the no-fly and selectee list practices of vetting 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.

Central issues surrounding the use of terrorist watchlists in the aviation domain that may be considered during the 113th Congress include the timeliness of updating watchlists 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.[14]

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 threat was brought into the spotlight by the November 2002 attack on a chartered Israeli airliner in Mombasa, Kenya. In 2003, then-Secretary of State Colin Powell remarked that there was "no threat more serious to aviation."[15] Since then, Department of State and military initiatives seeking bilateral cooperation and voluntary reductions of man-portable air defense systems (MANPADS) stockpiles have reduced worldwide inventories by at least 32,500 missiles.[16] Despite this progress, such weapons may still be in the hands of potential terrorists. This threat, combined with the limited capability to improve security beyond airport perimeters and to modify flight paths, leaves civil aircraft vulnerable to missile attacks.

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 FAA certification of systems from two vendors capable of protecting airliners against heat-seeking missiles. The systems have not been operationally deployed on commercial airliners, however, due largely to high acquisition and life-cycle costs. Some critics have also pointed out that the units do not protect against the full range of potential weapons that pose a potential threat to civil airliners. Proponents, however, argue that the systems do appear to provide effective protection against what is likely the most menacing standoff threat to civil airliners: heat-seeking MANPADS. Nonetheless, the airlines,

[13] Department of Homeland Security (DHS), "DHS Now Vetting 100 Percent of Passengers On Flights Within Or Bound For U.S. Against Watchlists," Press Release, November 30, 2010.

[14] For additional information see CRS Report RL33645, *Terrorist Watchlist Checks and Air Passenger Prescreening*, by William J. Krouse and Bart Elias.

[15] Katie Drummond, "Where Have All the MANPADS Gone?," *Wired*, February 22, 2010.

[16] Ibid.; U.S. Department of State, Bureau of Political-Military Affairs, *MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense System*, July 27, 2011, http://www.state.gov/t/pm/rls/fs/169139.htm.

which continue to face economic difficulties, 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.

At the airport level, improving security and reducing the vulnerability of flight paths to potential MANPADS attacks continues to pose unique challenges. While major airports have conducted vulnerability studies, and many have partnered with federal, state, and local law enforcement agencies to reduce vulnerabilities to some degree, these efforts face significant challenges because of limited resources and large geographic areas where aircraft are vulnerable to attack. While considerable attention has been given to this issue in years past, considerable vulnerabilities remain, and 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[17]

Provisions in FAA Modernization and Reform Act of 2012 (P.L. 112-95) require that the Federal Aviation Administration (FAA) take steps to accommodate routine operations of unmanned aircraft or drones into domestic airspace by the end of FY2015.The operation of civilian unmanned aircraft 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 Federal Bureau of Investigation 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. The payload capacities of small unmanned aircraft would limit the damage these attacks could inflict using conventional explosives, but drone attacks using chemical, biological, or radiological weapons could be more serious.

In addition, routine operations of unmanned aircraft by homeland security and law enforcement agencies and others may be vulnerable to jamming or hacking that could result in a crash or hostile takeover, as command and control systems typically use unsecured radio frequencies. Some have recommended that that unmanned aircraft systems be required to have spoof-resistant navigation systems and not be solely reliant on signals from global positioning systems, which can be easily jammed.[18] While TSA has broad statutory authority to address a number of aviation

[17] Prepared by Bart Elias, Specialist in Aviation Policy, belias@crs.loc.gov, 7-7771; Jeremiah Gertler, Specialist in Military Aviation, jgertler@crs.loc.gov, 7-5107; and Richard M. Thompson II, Legislative Attorney, rthompson@crs.loc.gov, 7-8449.

[18] Todd Humphreys, *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*, Submitted to the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, July 19, 2012; U.S. Government Accountability Office, *Unmanned Aircraft Systems: Use in the* (continued...)

security issues, it has not formally addressed the potential security concerns arising from unmanned aircraft operations in domestic airspace.

While drones 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 B unmanned aerial vehicles (UAVs), and has ordered another 14, to augment its border-patrol capabilities. Operating within specially designated airspace, these unarmed UAVs patrol the northern and southern land borders and the Gulf of Mexico to detect potential border violations and monitor suspected drug trafficking, with UAV operators cuing manned responses when appropriate. State and local governments have also expressed interest in operating UAVs for missions as diverse as traffic patrol, surveillance, and event security. Some law enforcement and first responder applications of drones may be eligible for DHS grants. 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, several other 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 drones in domestic airspace.

The introduction of drones into domestic surveillance operations presents a host of novel legal issues.[19] Some argue that drone surveillance may infringe upon an individual's fundamental privacy interest protected under the Fourth Amendment. 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 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,[20] the Fourth Amendment offers fewer restrictions upon government surveillance occurring in public places,[21] and even less at the national borders.[22] 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 have been introduced by Members of Congress that would require government agents to acquire a warrant before using drones for domestic surveillance, but would create exceptions for patrols of the national border used to prevent or deter illegal entry and for investigating credible terrorist threats.[23]

(...continued)

National Airspace System and the Role of the Department of Homeland Security, Statement of Gerald L. Dillingham, Ph.D., Director, Physical Infrastructure Issues, Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, July 19, 2012, GAO-12-889T.

[19] *See* CRS Report R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, by Richard M. Thompson II.

[20] *See* Kyllo v. United States, 533 U.S. 27 (2001).

[21] *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)).

[22] *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.").

[23] H.R. 5925, S. 3287, 112th Cong. 2d Sess. (2012).

Transit and Passenger Rail Security[24]

Bombings of passenger trains in Europe and Asia in the past several 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. 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, and Congress has provided grants for security improvements to intercity buses. But the number and operation characteristics of transit buses make them all but impossible to secure.

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

- mitigate risks to high-risk/high-consequence assets;
- expand operational deterrence activities; and
- enhance information sharing.[25]

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

[25] Department of Homeland Security, Transportation Security Administration, *Surface Transportation Security FY2013* (continued...)

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), and its Visible Intermodal Prevention and Response (VIPR) teams conduct operations with local law enforcement officials, including periodic patrols of transit and passenger rail systems, to create "unpredictable visual deterrents."

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.[26]

DHS provides grants for security improvements for public transit, passenger rail, and occasionally other surface transportation modes under the Urban Areas Security Initiative program. The vast majority of the funding goes to public transit providers (see **Table 1**). The Transit Security Grant Program (TSGP) did not receive a specified amount of funding in FY2012, as Congress left program funding to the discretion of DHS.

(...continued)

Congressional [Budget] Justification, p. 14.

[26] United States 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.

Table 1. Congressional Funding for Transit Security, FY2002-FY2012

Fiscal Year	Appropriation (Millions of Dollars)
2002	$63[a]
2003	65
2004	50
2005	108
2006	131
2007	251
2008	356
2009	498[b]
2010	253
2011	200
2012	88[c]
Total	$2,063

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: United States 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: DHS, *Transit Security Grant Program FY2012 Funding Opportunity Announcement.*

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.

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, leaving funding to the discretion of DHS.

In a February 2012 report, the Government Accountability Office found opportunity for duplication among four DHS state and local security grant programs with similar goals, one of which was the public transportation security grant program.[27] The Obama Administration proposed consolidating several of these programs in the FY2013 budget. This proposal has not been supported by Congress in the appropriations process to date, though appropriators have expressed concerns 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.

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

Port and Maritime Security Issues[28]

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. policy makers is prioritizing maritime security activities among a virtually unlimited number of potential attack scenarios. There are far more potential attack scenarios than likely ones, and far more than could be meaningfully addressed with limited counter-terrorism resources. Two port security initiatives the 113th Congress will likely continue to debate are the 100% container scanning requirement and the implementation of a port worker security card system.

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.[29] DHS appears to favor pursuing 100% scanning only at selected overseas ports deemed high-risk.[30]

Major U.S. trading partners oppose 100% scanning. The European Commission has determined that 100% scanning is the wrong approach, favoring a multilayered risk management approach to inspecting cargo.[31] CBP has tested the feasibility of scanning all U.S.-bound containers at several overseas ports[32] and identified numerous operational, technical, logistical, financial, and diplomatic obstacles,[33] including opposition from host government officials.[34] Singapore decided not to participate in the test,[35] and Japan has also raised objections to 100% scanning.[36]

Transportation Worker Identification Credential (TWIC)

On January 25, 2007, TSA and the Coast Guard issued a final rule implementing the TWIC at U.S. ports.[37] Longshoremen, port truck drivers, railroad workers, merchant mariners, and other

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

[29] 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.

[30] Bureau of National Affairs, *Daily Report for Executives,* "CBP Focusing on High-Risk Ports for Overseas Scanning; Two-year Delay Likely," #55 DER A-3, March 24, 2010.

[31] 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.

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

[33] 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.

[34] Ibid., Appendix A.

[35] "U.S. Drops Singapore Scan-all," *Journal of Commerce Online*, September 3, 2008.

[36] "Japan Expresses Concern about U.S. Cargo Scanning Requirement," *Jiji Press English News Service*, October 3, 2007.

[37] *Federal Register*, v. 72, no. 16, January 25, 2007, pp. 3492-3604. Codified at 49 C.F.R. 1572.

workers at a port must apply for a TWIC card to obtain unescorted access to secure areas of port facilities or vessels. The card was authorized under the Maritime Transportation Security Act of 2002 (§102 of P.L. 107-295). Since October 2007, when TSA began issuing TWICs, about 2.1 million maritime workers have obtained a card. The card must be renewed every five years, so many workers must now renew their cards for the first time.

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. A worker pays a fee of about $130 that is intended to cover the cost of administering the cards. Applicants have been required to visit an enrollment site twice, once to apply for the card and provide biometric information and a second time to pick up the card and confirm identification with biometric information, although Section 708 of the Coast Guard and Maritime Transportation Act of 2012 (P.L. 112-213) changed the process to require only one in-person visit by the applicant.

The card uses biometric technology for positive identification. Terminal operators are to deploy card readers at the gates to their facilities, so that a worker's fingerprint template will be scanned each time he enters the port area and matched to the data on the card. However, despite a statutory deadline of 2009 for issuance of a final rule on card reader deployment, TSA has not yet determined what kind of card reader technology to require.[38] In the absence of card readers, the card is currently being used as a "flash pass," and the biometric data on the card are not being used to positively identify the worker. It could be at least another year before a final rule is issued on card reader deployment.

In addition to delays with the card readers, questions have been raised about the worker screening process. A 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 keeping unqualified individuals from obtaining access to port facilities.[39]

Author Contact Information

David Randall Peterman
Analyst in Transportation Policy
dpeterman@crs.loc.gov, 7-3267

John Frittelli
Specialist in Transportation Policy
jfrittelli@crs.loc.gov, 7-7033

Bart Elias
Specialist in Aviation Policy
belias@crs.loc.gov, 7-7771

[38] Section 104 of the SAFE Port Act (P.L. 109-347) set a deadline of April 13, 2009, for the issuance of a final rule on card reader deployment. See U.S. Congress, House Committee on Transportation and Infrastructure, *A Review of the Delays and Problems Associated with TSA's Transportation Worker Identification Credential*, 112th Cong., 2nd sess., June 28, 2012.

39 GAO, *Transportation Worker Identification Credential—Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, May 2011, GAO-11-657.